Brandon Scott Krapf

US Army Intelligence, AFRICOM DET 1

Counterterrorism & Counterintelligence Section

I.S.I.S.

Interactive Synergistic Intelligence Superorganism

The future of the intelligence community's counterterrorism operations will be defined by its paralleling of current and prospective commercial applications in information technology. Where we are going we are already headed. Social open source resources are advancing to the point of being able to collect intelligence remotely, in real time, from anywhere, at anytime, in a multimedia environment. This information can be catalogued and searched using any parameters and the results represented in any way desired. This is reaching the event horizon where all of real world existence is to be simulated in a virtual reality where reality can easily be deconstructed into datastrings and analyzed in any fashion by feeding the data into particular inputs and applying specific algorithms or search criteria in order to receive on the other end an output of your choosing. The intelligence community needs to begin mirroring this social-technology for the purpose of effectiveness. The future 'system' that is proposed below is less of a system and more of state of being; and that state is called ISIS.

As the world becomes more and more connected and linked within itself between inter and intra networks; there becomes codependent sensitivity emerging that has not been seen since the evolutionary development of primordial bacteria. This connectivity is unwaivering in its growth and is going to occur whether global citizens want it or not. The issues at hand here is that the playing field will become level between the current actors of power and those actors whom hitherto retained very little power or influence outside of their kingdom or village.

September 11th 2001 showed the world that the disconnected or at least representatives of the disconnected finally had acquired the capacity and fortitude to influence and the connected states of the first world. As disheartening as it is that this lesson had to be learned vis-à-vis a negative impact, in the long run this will benefit the global community as globalization and connectivity has become an unstoppable force.

This materialization of this energy however has particular ramification if not harnessed and observed appropriately. Never before have events in one seemingly trivial and miniscule part of the world been so effective and influential in another part so far away. No longer can we ignore events based off their location. Historically geography was the key foci and center of gravity for all global events, conflicts and situations. Immediacy and simultaneous occurrence is what will rule the proverbial land. What occurs in what place will simultaneously occur everywhere at the same time.

This lack of a gap or stand-off distance to say the least is of crucial concern for those interested in retaining the security, safety and serenity that is known to typify most of the developed world. Thomas P.M. Barnett detailed this new dynamic of forces in The Pentagon's New Map. Barnett illustrates how the world has forged a new allocation of relations which is non-exclusive to any one actor. He defines three primary categories of geographic regions. There is the Functioning Core or known as simply the Core, which is populated by the majority of developed first world democratic societies whom retain an average state of stability. These actors are your usual members such as North America, Western Europe, Australia/New Zealand, a couple Far East Asian actors like Japan, South Korea, Taiwan and China. Virtually a few others outside of the typical geographic Core such as South Africa and Georgia.

The Non-Integrating Gap or the Gap for short, is the region that is populated by such unstable actors as Peru, Columbia, Haiti, and nearly all of Africa, Central Asia and South East Asia. The Non-Integrating Gap is characterized by its refusal to abide by certain rules sets that have been implemented by the Functioning Core and are based off the desire to retain security and safety while balancing the ideals of individual and collective liberties and human rights. To simplify the process of definition, basically Barnett took a map of the world and drew a line around all of the areas where United States military operations had occurred since the fall of the Soviet Union in 1990, and up until Operation Iraqi Freedom in 2003.

Barnett's original work is somewhat outdated now, and shows us how easily those who are along the Boundary of the Non-Integrating Gap can easily slip into the messy chaos that often consumes and defines the Non-Integrating Gap. Most notably, while reviewing the map you will notice particular actors who are located within the Functioning Core, yet have since the map's inception, have experienced at least one period of severe instability or who are currently in a period of instability. These actors are Mexico, Georgia, to some degree the Ukraine, India and China.

China as a state is easily considered a member of the Functioning Core, however it can be viewed often at times the rebellious brother in the family who albeit doesn't destroy the family, does often push the limits very close. Aside from China as a state, there is some serious concern about its western borders where there has since been a significant increase in upheaval and terrorism. Georgia presumably faced a one time period during its brief conflict with Russia, thought it is doubtful that will occur again, at least in the same degree.

India is another state where although it is included is easily on the brink of not being included due to its Kashmir issue, meddling with Pakistan, unwillingly harboring terrorists with connections to Al Qaeda and Pakistani Taliban. Also India has Sri Lanka on its southern flank in which it is still undecidable if stability will retain since the last major offensive against the LTTE. There is also that little problem with the Red Corridor.

Mexico is of particular interest because not only is it one of these actors that lies on the Boundary of the Non-Integrating Gap; it does so on our border and currently has the equivalence of an insurgency going on. An insurgency based on greed as opposed to grievance, which has spilled over into the United States. This particular situation is very dangerous as unlike many terrorist or insurgent organizations who threaten us, the Cartels have a pre-existing social and financial network already established in-depth throughout our country. This gives them the ease of ability and infrastructure of capacity to move swiftly and rather undetectably back and forth across the Mexican-American border and to include all throughout our domestic borders.

It is with this state of affairs that we are in dire need of a highly effective, preventive and reactive intelligence apparatus. Our current intelligence community though often effective and successful within particular constraints and contexts, simply does not retain the capacity to monitor everywhere at every time with the capacity for global immediate response. Even with particular programs such as Echelon and what was Carnivore along with many other global collection techniques, the community fails to operate as a single organism. Instead it is multiple organisms that fall under a loose affiliation of bureaucratic guidance.

The singularity is near. A synergy of resources needs to occur in order to implement the destiny of intelligence collection, analysis and threat management faculties. No longer is there to be NSA signals intelligence behind the walls at Ft. Meade, or Order of Battle scenarios buried in the hard drive of some ELP at the DIAC. A new system of collection and analysis has begun to grow, more or less on its own with little guidance and basically by way of evolution. This new system will be a system of process and practice as well as a legitimate software program. Perhaps it will be many programs tied together in a network sense. For the sake of simplicity, this system will be called I.S.I.S. This system will be radically different than what we have seen before. This system will be the product of millennia of research and learning. It will be less of a system and more of a superorganism.

This superorganism will be a system unbound by individual bureaucratic organizations, which is less of a system and more of the sum of its parts. Think of this like how first there are individual computers dispersed around the globe; then arrives Local Area Networks and intranets. Then these networks are then connected to each other creating a greater network of networks called the internet. As these individual users interact through this vast complex array of various networks and subnetworks there becomes a hypothetical 'cloud' if you will. This is why when you upload files to your Google Documents, it is said to be in the Google 'cloud'. In a way the grand network becomes its own entity, its own organism, and this organism's highest faculty is the cloud.

There is a striking parallel here, between a network being greater than the sum of its parts and studies of consciousness in neuroscience by quantum physicists. In The Physics of Consciousness, Walker calculates mathematically through quantative analysis how much data the human brain receives via its input portals and how much data it can actually perceive. He also goes on to methodically calculate how in the science of physics, particular elements and their interactive behaviors can create an externality that is greater than merely the two individual elements. In college students terms: two coeds in bed each with body temperatures 86.7 degrees suddenly realize their body temperatures have increased, at least perceivably.

This system will be the product of a fundamental understanding. One that can be summed up by the description of another system in yet another field: "the philosophical implication of quantum mechanics is that all of the things in our universe (including us) that appear to exist independently are actually parts of one all-encompassing organic pattern, and that no parts of that pattern are ever really separate from it or from each other." This system will exhibit more characteristics of a super organism than anything else. In order to typify the precedent of intelligence in counterterrorism operations as a superorganism we can look to the studies of superorganisms within the natural sciences. A review of these fields finds that "[t]he evolution of superorganism proceeds by a clash of force and inertia. The environment presents to the species particular problems and opportunities" (Holldobler & Wilson).

Cross-adoption of theories and practices is what is truly defining this system. It takes from all fields of knowledge. A root concept that will be incorporated is that "predictive synthesis, [which is] the ultimate goal in science" (Wilson) needs to become achievable. The community will be forced to find methods and processes that are found in other branches of learning that can be applied to the intelligence and counterterrorism fields. In Edward Wilson's book "Consilience" he delves in depth on the history, processes and benefits of cross-adaptation of the fields of knowledge.

On a micro level particular areas of the community to include security, defense, counterterrorism, intelligence and counterinsurgency have already begun incorporating cross adaptation and cross adoption. The wars in Iraq and Afghanistan have forced us to review our methodologies and consider nontraditional approaches to traditional problems. For example U.S. forces have realized that success by brute force only is not possible. A comprehensive understanding of the local population and its culture is needed to facilitate in their transition from one ruling body to another. One method of understanding the local population is to incorporate anthropology into the equation. The U.S. Army developed an anthropological program whereby they bring trained and educated teams to the war zone called Human Terrain Teams. These teams are the product of realizing that historically military strategy focused on physical terrain and that now within the sphere of counterinsurgency operations that the people are the terrain (Marlow). Now combat commanders take into consideration when conducting operations the intangible factors of social culture.

On the macro level the community seems to only be starting this fusion of knowledge fields. The community needs to be open to nontraditional methods of collection and analysis. Much in the field of study on defining consciousness affords us some abstract guidelines. One thing we have learned from this field is that "we have arrived at a science that has no entrance requirement, that excludes neither the subjective nor the objective, neither spirit nor matter, and thus is able to integrate the deep dichotomies of our thought" (Goswami). It is this breaking down of boundaries that is needed in the community.

This type of thinking is what will bring the Bill Gates into the community. The need to start insourcing innovation by bringing in experts from other areas of study outside of intelligence and counterterrorism and present them with the problems at hand and afford them the resources to collaborate for a solution. A perfect example of this cross-field collaboration can be found in the book "Complexity". The book details a story of how some of the greatest minds of the various fields of the sciences came together at the Santa Fe Institute to find similarities between their fields. What they found is that the rule sets, formulas and truisms in one field were perfectly applicable to the other fields (Waldrop).

Once the data inputs were stripped from the equations they discovered that the formulas and rule sets were the same. For example, in economics they found that A + B = C. Within the economic field the A might be income, B would be Debt and C would be your net worth. Once compared to physics the finding was that the field of physics also had a rule that said A + B = C whereas A was the electron number, B was the Negative charge and C was the overall charge. What this tells us is that a particular number of laws rule the universe, these laws are not bound to the physical sciences and often one field may have discovered a law that has yet to be discovered in another field. If the representatives of all the fields collaborate it is found that the fields will mutually benefit similar to the rule of comparative advantage in economic theory. The community can benefit from incorporating comparative advantage (Waldrop).

Quality <> quantity

Historically, there has always been a non-permeable wall between quantity and quality. A number is a quantity. A number of people is a quantity. A village in Somalia has 361 residents. This is a quantifiable number. You can calculate it, add to it, subtract from it, and perform a number of various functions with this number as it is a quantity. Quantities do not have breadth or intangible value. They are hard numbers that someone can state, that are irrefutable unless another person can prove a fallacy in the calculation of the equation. The generally viewed opposite of a quantity is a quality.

A quality is something of intangible value. Good, bad, indifferent. These are all qualities. Qualities are not considered measurable. They are considered emotive or felt, and expressed through language, and a lot of it, which is highly unlike the number two. Scientists and mathematicians have always been able to find truisms and formulas and equations that hold true in the quantifiable universe. While the social scientists, psychologists and political scientists were left with qualities that were much harder to manipulate in the sense of quantities. This is less so the case at present.

Social scientists have managed over the years to find – albeit often arbitrary – values to give to qualities, often in the sense of rating schemes. Once the scientist can apply a quantifiable quantity to a quality they can then in theory compute equations and calculate formulas. Walker manages to find quantifiable values to seemingly undefined qualitative measures such as vision. International relations scientists are able to apply values to possible outcomes of socio-politic-economic scenarios and games. In fact all of economics is less about calculating numbered amounts of money and more so about appending values to seemingly priceless qualitative items such as preference and choice. Much of economics is about game theory, which is the application of values to options or potential choices.

Let us explain this in a simpler manner vis-à-vis a brief anecdote. Once an economics student and an international studies student sat down to discuss economics. This conversation turned into including the topic of terrorism and more particularly suicide terrorism. The economics student insisted that the Buffolo 6 were illogical in the sense that they were each making approximately $150,000 a year and living comfortable uppermiddle class lifestyles in upstate New York. The student argued that their choice to kill themselves in a suicide operation was an unreasonable one that did not include the calculation of economics. The international studies student argued back saying actually the decision was completely economical, rational and reasoned. The economics student asked for an explanation of how this was so.

The international studies student then took a piece of paper and drew a line down the middle. He wrote at the top of the paper “Opportunity Cost of a Terrorist”. He then wrote the letters “A” and “b” and next to them each a choice that the suicide bombers had. Next to “A” he wrote “Live: $150,000 a year”. Next to “B” he wrote “Die: Paradise”. It would seem at first that the salary of $150,000 is a quantifiable value whereas the result of “paradise” was qualitative and invaluable. However, the student then took a leap of faith in how paradise could be defined. He went on the internet and found an advertisement for an escort willing to sell her virginity.

The student then multiplied that number by ninety-nine, for ninety-nine virgins. The number equaled $1.8 million. The student then went to a popular travel agency website and checked the cost of a flight to Bora Bora with one year of car rental, four star hotel resort with all everything included. Once the student added up the cost of this proverbial ‘paradise’ he came up with the numbered value of approximately $180 million a year. He then explained how economical it was for a terrorist to choose a life that would normally cost him $180 million a year to live, over a life where he made a meager $150,000 a year.

Surely, this is a rough and not entirely factual analysis, however it proves a point. The point is in this case that just because preference is a quality that is probably impossible to calculate, that in no way it means that what the preference is for is incalculable and in turn unquantitative. To the contrary the values need only be translated to their relative quantitative attributes. With this said, the intelligence community needs to draw more on the social sciences and their research into turning qualitative data into quantitative data. Once the community sees this as a valuable resource their ability to produce predictive analysis will increase many-fold. There are examples of how this can be done.

One example where setting the relationship between quantitative data and qualitative data as equal is with local population emotive properties. Human intelligence teams when operating in conflict regions often collect information on the population as a whole. They are interested in whether or not the local population is, for example, pro-American, Anti-American or indifferent. This is very important data to have, as it helps commanders decide where their forces and efforts should be focused (or extra guarded) for the sake of a winning the hearts and minds campaign within a counterinsurgency operation. Instead of analysts merely applying a colored map overlay of white, black and grey in order to differentiate the popular sentiment, these values could be afforded numerical values that then become something calculable.

Something that can be ran through formulas and equations and compared to historical data in order to create a predictive analysis. In doing so, the analyst can judge relatively accurately, whether or not a certain region is more or less likely to be harboring adversaries, or if they are more likely to commit to violent resistance. This analysis can also be used to judge which populations may be more receptive to an American presence or their likelihood of collaborating with American forces. The system will do this automatically. It will take the reporting from HUMINT general elicitation and targeted reports about particular towns and cross-reference it with the number of attacks in that area combined with reports from the respective Human Terrain Team Analysts. We must grasp the abstract concept that "an approach to this vast problem is gained by the analysis of the behavior of the individuals which constitute the economic community" (Von Neumann & Morgenstern).

Immediate and instantaneous communication will be the grease on the gears of the system. Superorganisms are known to have highly effective mass communication and collaboration capabilities. Every piece of data will be collected instantaneously, and from everywhere as the system will be an omnipresent one; it will be empirical. The defining characteristics of the system will be its sensor heavy attributes. It will retain a distributed collection apparatus that is everywhere at all times. It will not be bound by the traditional walls of classified and unclassified open source collection methods. When an operative is interested in a particular Madrassa in Indonesia that may be being used at night as a meeting site for Jemaah Islmaia, the system will not limit the datapool to CIA Wire reports, instead it will pull up all Youtube videos that have been geotagged at that location, and it will find every Facebook profile connected to that school, and it will be able to at the same time pull up the utility bills from the past ninety days and look for spikes in electrical and water use during late night hours. It will take the Youtube videos and scan them with facial recognition technology in case some video happended to catch a known terrorist in a video. It will take the facebook profiles connected to that school and will traceroute them to the children's parents using the childrens last names. It will then trace those parents names in its wikibase and retrace any other their connections. It will then be able to give a degree of separation between a six year old girl who attends that Madrassa and five degrees of separation away to Hamburg where a radical cleric writes an internet blog chastising the British forces in Afghanistan.

Bottom up approach

Our collection efforts have historically been based off the top-down approach. This is due to the nature of government affairs and political bureaucracy being the primary consumer of intelligence; however as modern, or more appropriately, *post*-modern warfare evolved into what we are currently facing whereas now we engage in a Captain's war, as opposed to a General's war. We face a global counterinsurgency effort, which we may aptly refer to as G-COIN. However, we must not limit ourselves to believing that the endgame is 'winning' this G-COIN which is essentially Oversea Contingency Operations. The COIN aspect is merely a means to an end, the true end being stability. With this in mind we must view our operations *not* within the context of war, instead within the context of *everything else*. Whether conflict comes from greed or grievance does not matter in the macrospectrum. Both motivations need to be addressed and inevitably neutralized. However in doing so we must comprehend the larger social paradigms that exist in this dichotomy. We need a bottom-ip approach for our intelligence collection.

A bottom-up approach to intelligence collection (and analysis for all intents and purposes) is to be based off emergence theory and the dynamics of complex adaptive systems. What this will inherently look like is somewhat fuzzy at this time; however what it will produce is far from misunderstood. Collection needs to not follow the traditional routes. Much how in computer networking there exists a concept of evolutionary routing; we too must adopt this notion. Evolutionary routing is how the routings network develops, in theory on its own accord in the sense that it detects the best possible avenues of approach. The network administrator does not dictate what works; instead the network dictates what works.

This concept is within a similar framework as the center of gravity notion is with conflict management and counterinsurgency operations. The intelligence community needs to end its view that it knows where intelligence is to be found. We need to let the intelligence *route* its own avenues of approach and we need to observe this and follow in suit. We must follow the people, the chatter, the masses, the information flow and mostly the interactivity of all of the above. We need to crowdsource our collection sources out to all elements, as often one word from twenty people is better than twenty words from one person.

Here is a brief anecdote to illustrate this concept. Two old friends are talking on the phone. Neo explains to his friend Jack how easily it is to collect information on people via open source networks. Jack then confesses to Neo, that Neo is the sole reason that jack avoids as much online activity in order to avoid any form of collection on him. It is then that neo explains to jack that no matter how hard or good he hides off the grid he still must interact with his environment. Perhaps jack takes his girlfriend to the movies Saturday night. Jack doesn't want anyone to know he went to the movies so he tells no one. However what Jack fails to realize is that his girlfriend has left traces in public for anyone to read into. She updates her Twitter account for example saying how she cannot wait for "popcorn and soda". The next day Jack's girlfriend's best friend writes on her let's say Facebook wall for example asking her how the movie was. Jack's girlfriend responds back with "it was great until Jack spilled the soda on my seat". This is a brief example in comparison how in the social networking realm, just how in the real world realm the chatter from others around you easily give off information about yourself whether you notice it or not. The system will pick up on these items and will calculate and archive them into its wikibase.

APPLICATION TO COUNTER TERROR OPERATIONS

As the counterterrorism community renovates its intelligence resources for the purpose of identifying potential terrorist threats, neutralizing them, and ideally retaining the capacity to result in predictive threat analysis. The innovations in counterterrorism tactics, techniques, policy and procedure that have been spawned form the necessity to counter a threat type unlike we have seen before will provide the needed platforms for countering future threats. What is needed is a global predictive, detection and response system that is not bound by space or time. This system needs to be respectful of the need for conducting such operations within the context of a global environment. We need to be able to detect a threat of distributed denial of service (DDS) against a local America internet service provider near Fort Meade coming from Guatemala while simultaneously detecting a vehicle Bourne improvised explosive device (VBIED) about to be detonated outside a U.S. military base in South Korea – and all at the same time.

Upon detecting these threats there needs to be an immediate response element that can neutralize the threats with immediacy. If for example we neutralize the DDS threat, we need to do so without disturbing the surrounding environment – i.e. disrupting internet connectivity. In the case of the VBIED we may need to neutralize the threat by way of detonating the VBIED before it reaches the front gate of the base. Consider technology that could scan the dynamics of the upcoming vehicle and cross reference it with the number of passengers and expected weight with the actual weight of the vehicle. The system would be able to tell if there was a considerable amount of extra weight and in turn queue nearby chemical sensors to detect potential explosive traces on the vehicle. While doing this the license plate number would be read and cross referenced with a residence address that is found to belong to an individual with suspected ties to terrorist activity. Within minutes a Predator drone would be deployed to engage the VBIED.

Minimizing collateral damage within the global environment is a vital necessity. The defense community has realized that renovations in response tactics and platforms are needed and have begun implementing needed changes. For example with conducting drone attacks in populated rural or urban areas we have learned that the explosive payloads used with our weapons platforms are generally not conducive to conducting surgical strikes (Hodge). Reducing collateral damage is all part of the need for operations to attain a global response capacity. Being able to strike anywhere in the world within minutes is pointless if scores of innocent civilians are killed in the process. This is relevant to Barnett's concept of conducting operations within the context of everything else. This global response capacity is seen in the Pentagon's endeavors to find ways to launch UAVs anywhere in the world within an hour and retain the ability to stay on target until subsequent responses are available (Weinberger). This decentralization of operations is what is needed in order to combat the decentralized methodologies and dynamics of the threats that are faced currently and more so in the near future. The need to essentially *become* the enemy to combat them is a crucial tenet to the future of intelligence in counterterrorism.

Practice

The first thing that is needed is to be sure that all classified data on our internal systems and networks are either moved to or linked to a central database. This way there is a single archive of all intelligence that has been collected to date. Then all other open source data needs to be indexed and archived from all that we have available. Thereby creating an archive of all existing information available in the world. From there the system can begin adding all future streaming data. Understandably so, there are and will be issues with language translation between differing programming languages and system compatibility in general. These issues will just take time and effort to work out.

A critical issue however exists with having a single database for searching content. This issue is with the ability to search all data at all security classification levels. This issue has troubled the community for some time. It becomes too much of a burden for a user to search the Top Secret database, then the Secret database, then the Sensitive database and then the open source. Due to the nature of the networks being separated this poses a problem for datafusion. One possibility would be to in effect ‘carbon copy’ all intelligence into the higher levels of classification. For example the Top Secret network would receive a copy of all things Secret and below. This unfortunately would bring a great burden on data processing and storage. However, having faith in the comparative advantage rule to work this out is probably the best available solution currently.

Database vs wikibase

In general a database is a one way semi-closed system. The user enters a data string which is then stored in the database wherein later the user can recall that datastring. Databases however have become more versatile over time in the sense that the user can input multiple values and can even change multiple values of individual or several records. The problem with databases in a net-centric world is that networks live, breathe and adapt along a timeline. They are not static. Whereas, for all intents and purposes, databases are that of a static quality. The system will operate differently than a traditional database. Instead it will utilize a wikibase. One that is accessible by all users at all times from any angle and completely manipulative. Users can change data continually. Rest assured, this data has to be cited and whoever began the original informational thread along with all others who have added to it, they will be informed of the addition so they can confirm or deny its validity.

TECHNOLOGIES

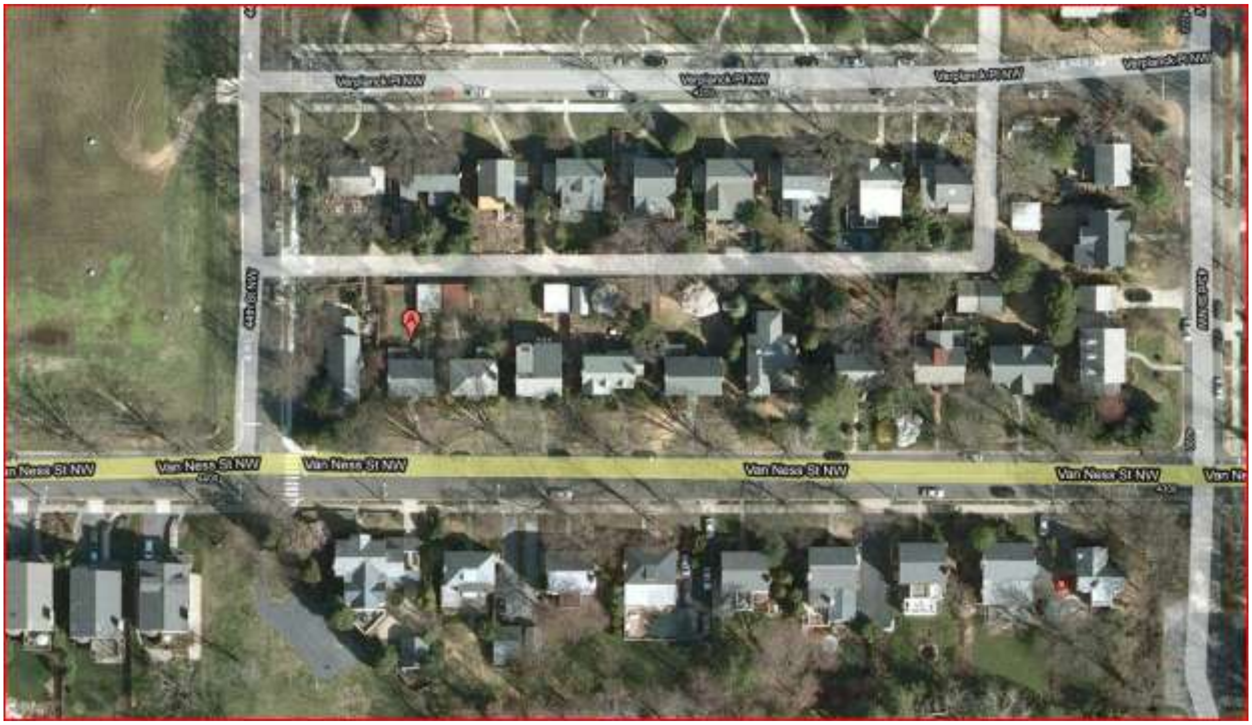
GEOLOCATION OF WIKIBASE

Once all the data up has been archived up to the present, it is to be overlaid via Geographic Information Systems (GIS) modeled applications. GIS are computer programs that allow for graphics overlays, such as maps, to be superimposed over a plane along with other graphics using special oriented algorithms for geopositioning. This type of technology is just becoming a popular tool to be applied to open source coding, social media, social networks and a slew of other applications available for the public. This technology has given birth to a new subfield of conceptual applications such as GeoLocating, GeoTagging, and GeoTargeting. The possible intelligence use of this is unfathomable. Enter the world of GeoLocation; where you can stream through multimedia and blogs and social networking sites all tagged to a geographic location.

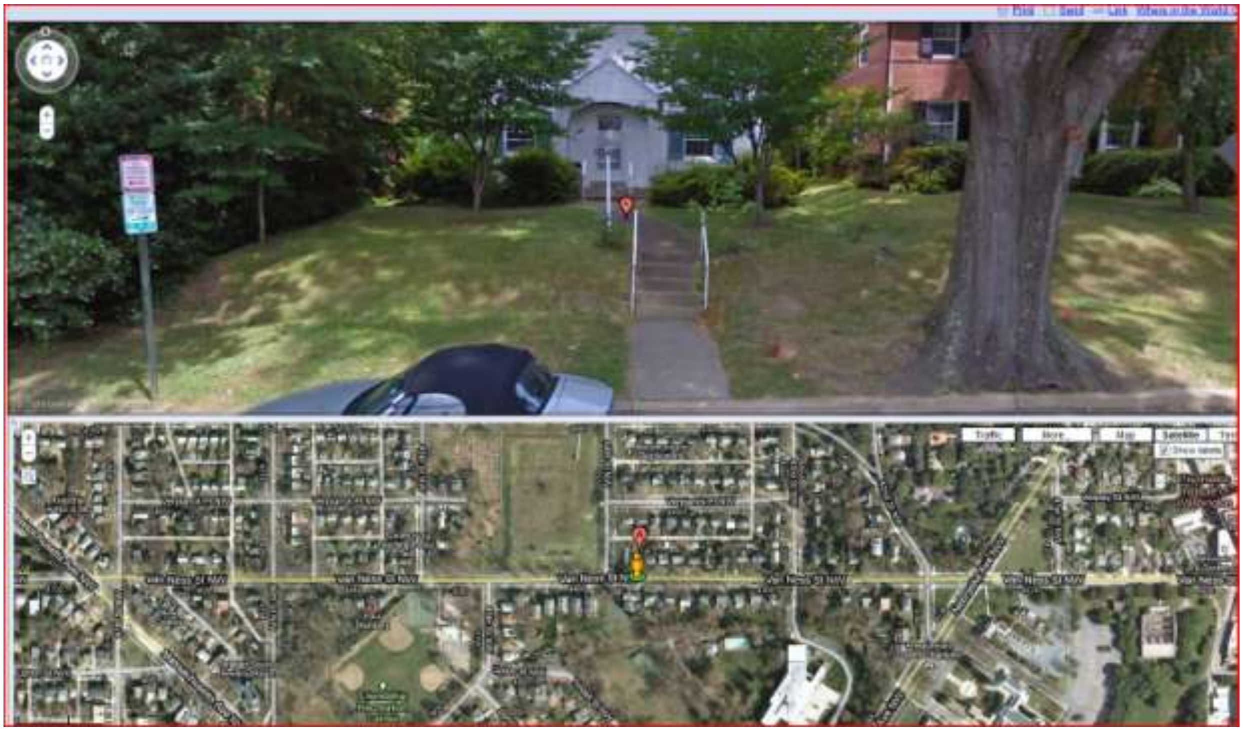
Map
Satellite
Terrain

This has already been done in the intelligence community to a decent degree. However it is generally just target specified datasets. For example if a military commander on the ground is in charge of a particular Area of Responsibility (AOR) then the intelligence analysts that work for him have probably created overlays for maps and power point presentations, and more recently created overlays for a classified equivalence of Google Earth. This is simply not enough. This needs to be applied to the entire world and to include unclassified open source datafeeds.

If the user wants to review a particular area that a raid is going to take place in 24 hours out, they should be able to view this graphically with full multimedia capability. In the unclassified world, if I would like to review a location that is perhaps not available for a physical reconnaissance, I can do the equivalent of a map reconnaissance via Google Earth which adds full multimedia capabilities. Sure there are static data sets available such as still photography and general map data. For example let us review the following image of a particular residence in Washington, DC.



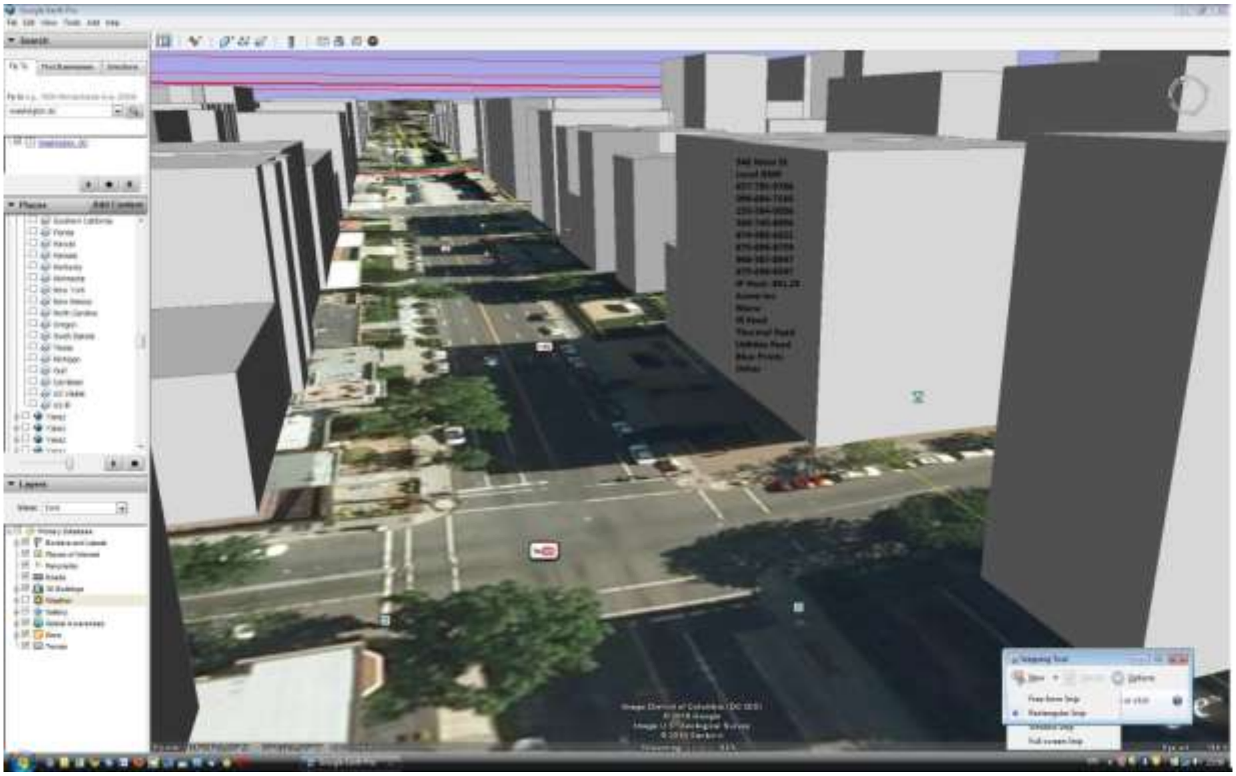
This image from Google Maps is equal to what most satellite imagery will show you if you are trying to view a particular location. Unfortunately there is not much that can be taken from this image aside from the two dimensional data albeit is useful for a tactical team to raid the house, frankly it tells you very little outside of that. Other pieces of information would be of much greater use. Surely many a raid has on a target's house have blundered due to the simplicity of two dimensional imagery. However there is something else that is available that has yet to be implemented across the intelligence community. Google refers to it as StreetView.



What Google's StreetView has done is have vehicles with cameras on their roofs drive down every street in America and a few other countries and take photography from the street level and have meshed it all together in order to create 360 degree views as if you were on the ground in front of the location in which you were viewing. The zoom function is workable so you can even zoom in on whatever you are looking at. As is apparent, there is a significant increase in available data or intelligence now available for this particular location. You know what the obstacles are around the house, the color of the house, the surrounding details, and depending on how well the imagery is, the user can tell which way the door opens, amongst other things. It is possible to zoom in on with StreetView and even make out the outdoor cable box on the house so the user can know what cable (and presumably telephone and internet) service the target's house uses. The applications of this as an intelligence tool are endless.

Now imagine that the exact grid-coordinates are available for this location and the location happens to be the residence of a high value target. With a simple unmanned aerial vehicle viewing from above to confirm thermal and infrared data to conclude the presence of occupants within the residence and there is authority granted for lethal action then this becomes a very useful observation tool. However, now view this as an interactive tool. Consider the potential for unmanned aerial vehicles or satellite thermal feeds linked to the application. So as the user navigates though the Google earth type application with a StreetView type technology there could be a constant feed in the bottom right of the screen showing thermal or IR activity. Now let's conceive the possibility that with a simple right hand mouse click on the residence a table of options presents itself. The list of options could be as such: Bookmark, Tag (with a keyword or name), audio (all landlines and cell/sat phones within the residence are then streamed live feed to the user through their speakers), RFI, (Request For Information, ie further data available) and Engage. If the user selects *engage*, then the Predator drone flying above feeding live thermal or IR to the user, which happens to be equipped with a Hellfire missile, suddenly and undetectably releases its payload into the target location. Boom. Instant Bad Guy Be Gone: Just add Google.

The above graphics technology is available via the simple Google Maps web resource. However with Google Earth –which requires a download of the software – there are many more features added that give the intelligence community endless opportunities. The image below is an image of downtown Washington, DC. There are many overlays available that a user can select to be applied while viewing the map. The most crucial of all is the option to show three dimensional buildings. A user can actually 'fly' down to any level to include street level and navigate through the streets as if they are flying around. This is only partially what is useful for the intelligence community. Consider all of the overlays and data available that can be geotagged and applied to the map. As the image shows, there are various Youtube videos that are connected to the location along with various other items such as Wikipedia links for relevant information, business listings for shops located there which the user can select and get further data on the businesses such as phone number, address, store hours and anything your mind can conceive.



Imagine briefly, if the images from the StreetView were applicable to the surfaces of the three dimensional buildings. This is not farfetched and if it has not all ready entered the testing phase it will shortly. A user could navigate to anywhere in the world, zoom in and see real world three dimensional imagery of any building on the face of the planet. With the advent of geotagging on every piece of communication and image that flows through the datasphere consider the ramifications of having this entire data flowing live stream and annotated upon the graphical representation of the earth. For example, the three dimensional building in the above photograph has a list of available data overlaid onto the side of the building.

This data is hypothetical and includes all the cell phone numbers that are currently present on the property that the building resides, the internet protocol (IP) address or host address that is linked to the building, the physical street address of the building and the name of the company the building is used by. There are of course further data sets that could be applied to the structure. This data would include, though is not limited to; the blue prints or floor plans of the structure, the feed for all utilities being used in the structure (for example electrical, water, phone, gas etc), the full company profile of the resident business(s), the list of names (and biographical data) of all employees registered at the business, the list of biographical data for all the users to any cell phones that are currently in the building, the financial records for all of the above, the criminal records for all of the above, the foreign travel records of all of the above, the ability to link or select further data on each individual piece of data reported.

For example the user could select the building, see all of the current cell phone users within the building at that time, and then select live audio feed to listen to any and all conversations currently in the process via the cell phones. The user could establish a 'filter' for a key word; let's say in Arabic, such as *khabeer bayt* or "big house" which conceivably could be the name of a safe house used by an Al Qaeda cell known to be operating within the DC area. When within any of these cell phone conversations –in real time- the key term or phrase is used, the 'filter' would alert the user of the occurrence. The user could then select the individual cell phone user whose connection the key phrase was stated in, could select a trace on the call which in theory would go back to a cell register to an individual named Salim, who based off trianglization or GPS within the cell (doubtful) to a small village in Tunisia. From there the user can slect the grid-coordinate of where Salim is using the phone, and upon doing that the entire Wikibase is queried for that location.

It will not stop there, however. If there are no hits (and even if there are) the system will volunteer other potentially related data, similar to when Google is searched for an unknown term and it displays a “Did you mean?” For example, reports that have been geotagged to the village but not necessarily that exact grid-coordinate. Also if there is no reporting data for that grid-coordinate though it has been queried previously the system will display that information and a point of contact for whoever had previously queried that datastring.

Where collection and analysis blur

Collection and analysis are considered two different beasts. However, with this system this is less so the case. The system conducts automatic analysis of all data entered. Being that there is a more or less live stream of global data it is less about data being entered and more about analyzing content flow. When the user is reviewing a particular item, such as a building structure all relative data will automatically be tagged and connected to that structure and most importantly it will be archived. So when the user is looking at this structure, much how old Youtube videos are connected to a particular location, so will all past data that was connected to the structure. The user could select the building structure, and instead of, or also to include, the user could utilize the same filter though for all past activity.

This process blurs the line between collection and analysis however does not discount the value of either processes or their necessity for the human element of analysis. It merely augment sand relieves the human analyst of a greater burden while acting as a force multiplier in order to maximize the user’s potential.

Collection

Remote Sensors

Remote sensors are not new and neither are unmanned ground sensors. The US military have been using unmanned sensors for decades. These sensors can be implanted in the ground, placed into the ocean, and even left to float in the air. This is all measurement and signature intelligence (MASINT) is. There are remote sensors also that come from satellites that orbit the earth. Unmanned aerial vehicles do basically the same thing, however are much more flexible as a platform, in the sense that they can be fitted with offensive kinetic capabilities. This is what has been being done in Iraq, Afghanistan and most notably in Pakistan recently. MASINT needs to expand exponentially, even faster than it currently is.

RFID

Radio Frequency Identification (RFID) tags are currently being used for many application in both the private and public sectors and the intelligence community has learned the use of these and have implemented this use. This implementation needs to increase drastically also. Imagine if the globe was covered in so many of these, either the passive or active ones. Anything and everything could become a trackable item. MASINT teaches us that everything leaves a trail either permanently or temporarily. What we can learn from this is that if any one thing remains motionless it still usually gives off some frequency or wavelength or pheromone. If something moves, then it definitely creates disturbances in various fields of either magnetic, atomic, radio or quantum etc. Every single thing in this world can be tracked. This needs to be done.

The Department of Homeland Security has already begun researching and promoting the use of RFID tags for the purpose of improving border security. The practical idea being that as far away as thirty feet before an individual reaches the border crossing point, they have already been identified (ALBRECHT, 30). RFID tags are already in use prominently in the commercial sector and many governments around the world have begun instituting - or at least preparing to – them in their national identification documents. China and Qatar are currently in the process of this implementation, and in America, the state of Washington has already issued out thousands of RFID outfitted driver's licenses, and the new version of the American passport has chips in them (Albrecht, 74).

The national identification cards that China is shelling out $6 billion on; are to be riddled with a plethora amount of personal biographic data "including health and reproductive history, employment status, religion, ethnicity, and even the name and phone number of each cardholder's landlord." This initiative will compliment the future of China's surveillance state (Albrecht, 75) which will inherently solidify a Huxlian (read: Brave New World as opposed to cliché 1984 references) world of surveillance and human cataloguing. This news is far from contemporary, as Wired Magazine reported back in 2007 that the endeavor will be "the world's largest effort to meld cutting-edge computer technology with police work to track the activities of a population" (Weinberger).

Utilizing RFID technology to track inventory universally as applied to humans is not illogical or far-fetched. It is fairly public knowledge that the military already uses highly accurate

GPS solutions for weapons and ISR platforms such as UAVs (Hambling, Shactman). In 2006 a patent granted to IBM titled “Identification and Tracking of Persons Using RFID-Tagged Items in Store Environments” annotates the possible use for tracking people in a “networked RFID” reader world. Reportedly these are called “person tracking units” and would be enmeshed in the fabric of the commercial environment. The RFID readers would be distributed within “shopping malls, airports, train stations, bus stations, elevators, trains, airplanes, restrooms, sports arenas, libraries, theaters, [and] museums” (Albrecht, 75). This is a MASINT dream come true, as if this concept was utilized by the intelligence community, every single person and in theory item, could be tracked and monitored. Imagine the possibilities.

Consider for a moment knowing where – in a conflict zone – every citizen was located in real time and being able to cross-reference that data with other nearby people along with cross-referencing the data with geotagged/geospatial location based intelligence. For example, one could virtually watch a local Sheikh suspected arms trafficking go to a police station to meet with the police chief then off to a local market and lastly making a pit stop at his village mosque before returning home to meet with his granddaughters. Now for a moment, take the dataflow and stream it into a Google Earth type application where every structure was tagged with biodata that was collected from all-source intelligence to include that of reporting Human Terrain Teams, Tactical HUMINT Teams, Civil Affairs Teams and any other relative sources.

Multi-Modal

The system needs to comprise of a multi-modal collections platform, incorporating all modalities of data production, one that is truly ‘all-source’. This is to include in theory a streaming data flow of all data emitted from around the world. No matter what the source of the data. Open source intelligence analysts consume endless hours of foreign radio, television and internet broadcast currently. There needs to be an initiative to computerize and automate this effort. All multimedia broadcast to flow into the system are then to be translated into English and stored after processing. This was there is an archive of every printed news article, radio broadcast, news television broadcast that occurs. In theory this could include published books also, though it must include scholarly papers for sure. Once this is digitalized it becomes searchable, to include affixing 'tags' on every item for example a scholarly work by a professor in Dubai who is writing about genetic manipulation would end up having his work tagged with 'science' + 'Dubai' + 'genetic' etc. This way the indexing of the data would be much easier to recall when the system is searching for keywords and data strings later on.

This multi-modal endeavor would also include all phone calls made, all VOIP communications, all emails, online instant messaging, cell phone text messaging and any other form of communications. All of these are to be translated, tagged, indexed and archived. This is like a global empirical equivalent of someone using Google Mail, where all of their emails are saved and labeled and can be searched later. Google Mail also does the same with all Google Talk instant messages. These all can be searched at anytime as they are stored permanently. Even communications via the program Skype, if the G-Recorder add-on is purchased, will store in your Google Mail every instant message and to include every VOIP phone call. Ideally all linguistic data such as words stated in all telecommunications and to include words in all photographs and video would not only be translated from their original language into English, but hypothetically into every language. This is particularly important as not every terrorist network speaks solely one single language.

The add-on application does not just register a call history, it actually records each call incoming or outgoing, who the call is to or from and before it saves it to your Google Mail it gives you the option to enter additional notes about the call. In theory if an individual only uses Google Talk and Skype for communications then at any moment all of their communications can be searchable, recalled, and reviewed by date, time, sender, receiver along with many other search options such as does an email have an attached file. Imagine if this Google Mail set up was applied to the entire world's communications. Imagine the amount of data there would be to sift through and how much information would be available. None of this would be deleted as months or years down the road there may be a connection made that was not noticed previously.

The system would not stop at just communications. The system would be doing the same with other disciplines of intelligence, not just signals intelligence. All intelligence reporting would be tagged and archived. Human intelligence reports, counterintelligence investigative reports, diplomatic cables, even the 'spot' reports or SALUTE (size, activity, location, unit, time, equipment) reports completed by the infantry soldiers on the ground in every conflict zone. The US Army began back in around 2005 a conceptual program called ES2 or Every Soldier is a Sensor. The logic behind this program was that human intelligence reports were just not enough to populate the data pool that filled the Priority Intelligence Requirements.

It was realized that one Tactical Human Intelligence Team collected in one city or province of Iraq was simply not enough eyes and ears to have on the ground. This needs to be implemented industry wide for all government employees. Every employee should be writing up reports or receiving debriefs of what they have seen. These reports all enter the system for processing. Perhaps some random US Army cook is tasked out in Afghanistan to operate the .50 caliber machine gun on a logistics convoy due to lack of manpower. If the cook sees anything it needs to be reported. Perhaps in 2004 if three different cooks on three different convoys had noticed Iraqi men in black clothes out in a field in Khan Bani Saad those three reports would have been sent up and a correlation would have been found and a patrol may not have been ambushed weeks later in that same spot.

The idea of having federal employees retain situational awareness and report anything of interest seems daunting as most people are not even close to being trained in what to look for. They all need to be trained in what to look for. This concept that only intelligence professionals are trained in these fields is an illogical one. Surely these non-intelligence personnel should not be out running their own source networks and conducting surveillance on their own, however they should be trained in key identifying factors and made aware of key foci of interest. This All Americans are Sensors or for short A2S if you will needs to include non official business to the full extent.

If a US Army Reservist decides to take a vacation to Egypt to visit his girlfriend there should be some debriefing of this. Perhaps the soldier did not notice anything because he was unaware what there was to notice. It would be disheartening to consider that the neighbor or adjacent building over form the soldier’s girlfriend’s apartment was under suspicion by CIA of being the residence of a known Al Qaeda operative. The soldier should not be told this before he goes as it would clearly be too dangerous, however the soldier should be debriefed, and his whereabouts abroad annotated as detailed as possible.

Consider the possibility that the soldier was able to give an exact location of his girlfriend's apartment that he stayed at, which could be translated into a 12 digit grid-coordinate or GPS specific latitude and longitude. Consider then that six months later the NSA traces a suspicious disposable cell phone call to in the vicinity of the same location. If there for whatever reason is not an option to acquire imagery of this area aside from aerial satellite imagery, or if the CIA cannot afford to detail an agent to ascertain some sort of bearing on the location such as what businesses are in the area, is it an ex-patriot friendly area, is it a commercial district, etc. Then the grid-coordinate would be entered into the system and this grid-coordinate would immediately pull up all other data from that location perhaps within a 500 meter radius.

Suddenly the analysts notice that a soldier had visited the area. This soldier then could provide all of his tourist pictures and camcorder footage and anything else. Most people, to include trained intelligence analysts cannot conceive the notion or at least to such an extreme, of how much intelligence is available or can be extrapolated from other data sets. The skill is in the detail awareness. You see a picture of a girl; you can only make out the arm of a man in the side view. Most dismiss that, however if you were to be looking at an entire set of photographs you may take notice that the man's wrist has a gold watch on it, and then later take not of the same gold watch in a seemingly other unconnected photograph.

A2S, would not only be focused on employees of the federal government. Clearly that candidate pool leaves a very minute pool of reporting data. Civilians travel all over the world to places that they either should not for their own safety, or to places that they do not know is a potential dangerous location. These civilians inherently and unwittingly produce more unclassified intelligence that the intelligence community could ever dream of. Why not search and save every bit of data on every single social networking site? Imagine if DIA was tracking a particular target, however they had lost him somewhere in Bangkok. Most trained operators, whether red force or blue force, are generally decent at threat recognition. This means they should be able to in a relatively quick period of time decide if a picture being taken in a city market is an undercover operator or just some drunken tourist taking pictures so as to later upload to his online Picasa album.

Herein lays the crucial concept. If the tourist takes a picture and the DIA target happens to be in the picture he will think nothing of it as the target will rapidly dismiss the tourist as a non-threat, which is semi-accurate. The tourist himself is of no threat. However within 24 hours his photographs could be posted to the internet yet you must have access to his account to see his pictures. This needs to stop. If the intelligence community was able to scan all of these photographs from everywhere on the internet and utilizing facial recognition technology – which, ironically the Picasa application has and uses when it scans you pictures –then perhaps DIA would have just been able to pinpoint the exact location of their target.

This concept seems unproductive at the moment whereas the hypothetical tourist may not post his photographs for weeks, months or years. However just knowing the target was there and at that time is still often useful intelligence, as further in time there may be a need to connect the target to perhaps an Abu Sayyaf meeting that occurred that time. Also, with the invention of instant uploading to the internet coming on many digital cameras and video cameras these days, this open source pool of intelligence is only going to become more and more useful and gain time sensitive accuracy. As technology advances with the geotagging of pictures, this will also drastically increase the usefulness of open source collection from social networking sites. Consider this collection effort as crowdsourcing collection inputs into the system.

Analysis

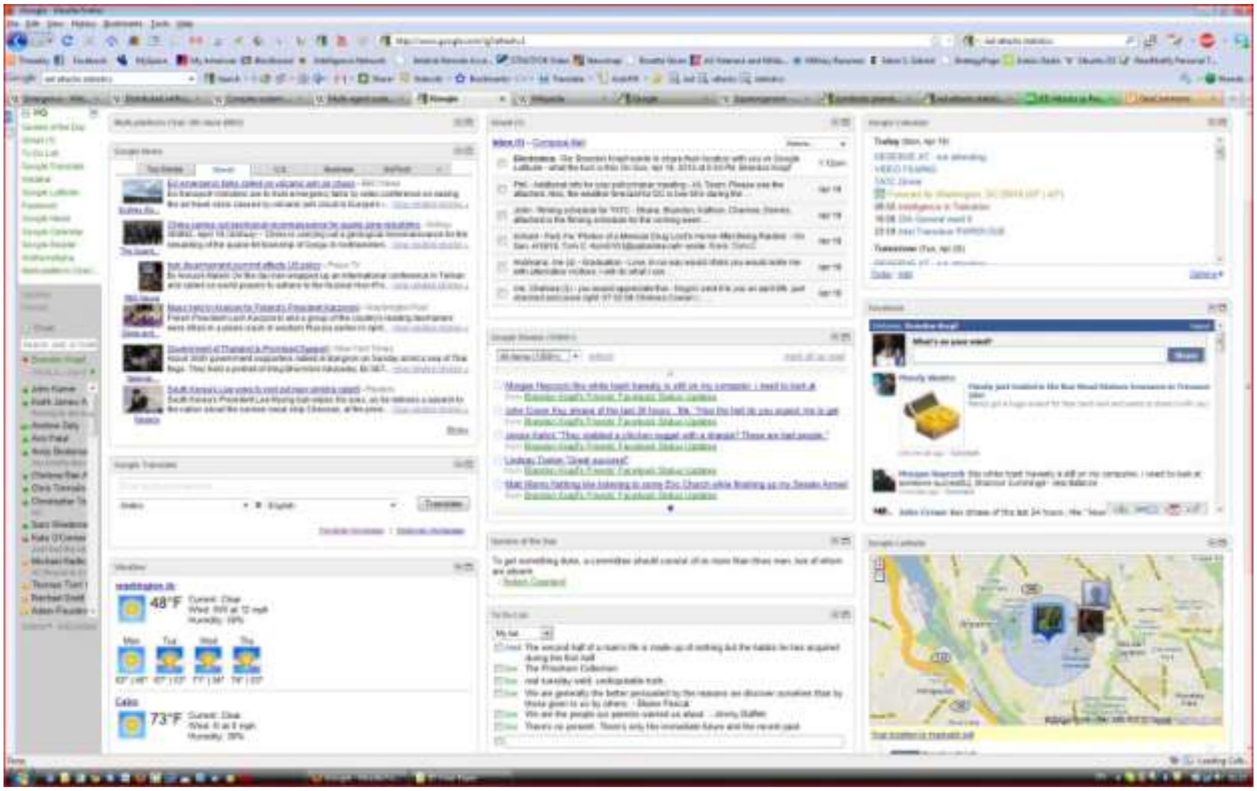
Think TAC or what was once Tripwire; but four dimensional and with automatic, adaptive, archiving abilities. Then include retroactive recall analytical capabilities. This system would not only limit its analysis to the current live feed; it would also include all of the historical feed that it has previously archived into its wikibase. The analysis process will utilize the multi-feeds that come in similar to how RSS feeds are transported into the likes of Google Reader or Yahoo Pipes. The single graphical user interface (GUI) makes it easy to manage an infinite number of data streams arriving all in one portal. From this point the user can observe, assess or react to the particular streams of interest to include filtering and search mechanisms. An example of a possible GUI is shown below. You will notice the multiple feeds from various sources, all subscribed to by the user dependant on preference and necessity.

The analysis side of the future system will not only operate more effective and accurate due to better collection and data retrieval; it will utilize what is already being researched. Computational mathematical algorithms are being looked at for their ability to supplement the human analyst. A new program called Aggregative Contingent Estimation (ACE) is in the process of testing its ability to calculate the accuracy of analysts' assessments. This is a form of competitive analysis of the analysts themselves. Utilizing statistical probability functions for assessing the analysts' predictions ACE is expected to be able to determine whether an analyst is likely to be accurate with their assessments of particular intelligence issues (Drummond 1). The future system will incorporate this methodology in its full-spectrum analysis environment.

The Pentagon has conducted research in the field of a artificial intelligence, with the application in mind of simulating the sensemaking systems of a human intelligence analyst. They held a conference where they detailed the potential for a new program titled Integrated Cognitive-Neuroscience Architectures for Understanding Sensemaking (ICArUS). The intelligence community needs to incorporate all the help it can with analyzing intelligence, especially with the future of such mass collective parameters coming to fruition. ICArUS and potential similar endeavors will help analysts greatly with assessing large pools of data and most notably, smaller low-level redundant analytical taskings. This method will free up further analyst resources for more crucial applications (Drummond 2).

With lower level tasks being left to automated services, analysts will be free to focus on their particular respective areas of focus. The intelligence community will see a restructuring of organization. Eventually the community will become a more unified *command*, while simultaneously resembling a distributed *node* or task force function. This is where the community becomes essentially a super organism; as it develops into a cellular nature whereas its production becomes greater than the sum of its parts. Each node will consist of its special area or issue of focus, and will follow that task in real time, with real world response capability. No longer will an analyst sit at a desk merely monitoring message traffic and summarizing the highlights.

The new analyst will operate within their respective node, yet may not be confined by geography. They will collaborate with their colleagues using an interface that resembles more of a digital graphical user interface. The user will monitor a real time flow of multiple sources feeds that are fused together right in front of the user's eyes. The user will track targets and retain the ability to engage them either directly or indirectly depending on the afforded guidance. The user will be able to identity and neutralize threats right from their desktop. This will be the empirical equivalence of a UAV operator sitting in a chair stateside while virtually hovering over Helmand Province in Afghanistan. In no way will the system completely remove the boots on the ground so to speak, nor the field agent running operations; they will merely augment them and facilitate in handling tasks that do not require face to face contact. Surely source operations and counterinsurgency operations will still require the human component of interaction, however many operational tasks can be completed from a distance.



This distributed node network will incorporate a form of distributed resource management. Crowdsourcing processes will be utilized in order to downsize the work load on any one user or system or network of users or systems. If a particular user is managing an increasing responsibility task while other are not, the system will redirect additional taskings to other users who may have less going on. This is the intelligence cycle in real time. Reporting, reviewing, requiring, retasking. This is 21st Century intelligence where there are no walls except the ones you imagine.

Evolutionary learning will be applied to all user behavior. The system will be reactive and adaptive to not only user input but will annotate, analyze, assess and act upon user behavior pattern recognition and analysis. Much how your web browser remembers you previous search string entries and offers them a options. In Neil Postman's Technopoly, he illustrates as far back as 1992 that information technologies like software need to, are becoming and will become, smartware. The programming will adapt to the user and will become a virtual extension of the user vis-à-vis preference recognition and implementation. As a whole the system retains its particular user feedback mechanisms that lead to low-level artificial intelligence by way of bottom-up approaches and reinforcers. There will be ‘feeds’ of data updates. Live realworld streaming info-feeds. Within the system all users have the option to “Like” any particular piece of data. This option is the process of reinforcers so as to reinforce the user that his work is appreciated and to keep doing what he or she is doing.

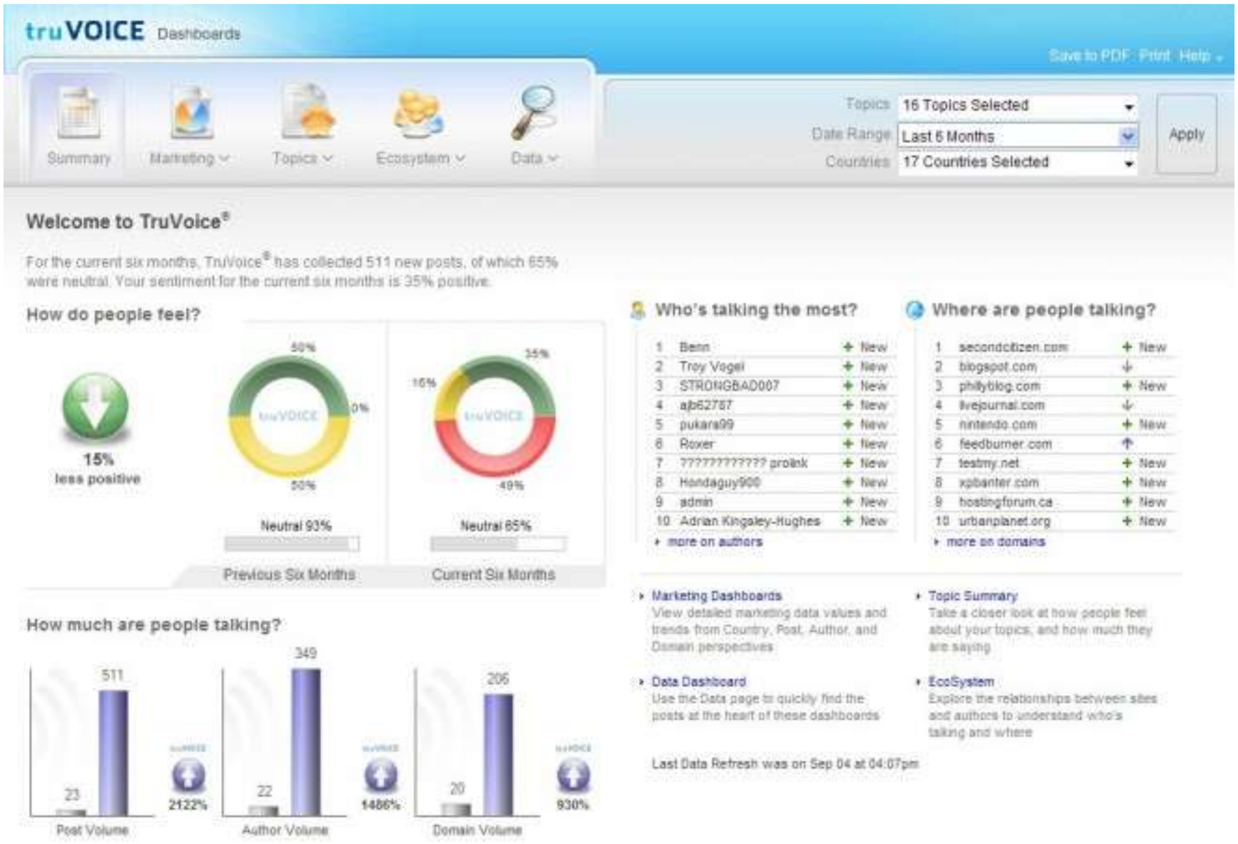
If a user in Molesworth, UK receives message traffic from a source in the Jordanian GIS that Mustafa Ahmed Ali Mohamed lives at grid coordinate WV 9482 7453, before the user can even blink the system has already updated its wikibase by linking the grid coordinate with the individual’s name. Upon this occurrence any other user will be updated in their respective feeds – assuming they have subscribed to something connected to any of the relative connected data strings (such as the name or grid coordinate). The feed, unlike Google Reader, will be more like the Facebook live feed, as in the user if they are receiving that feed (being that they are within that proverbial friends group or network) has the ability to comment on the updated information. The user can simply “Like” the report or they can comment on it, for example with a declarative statement like “this is a known AQAP hotspot” or a inquiry statement such as “wait, how long has he lived there?”

OPEN SOURCE

Open source intelligence (OSINT) has always existed in some capacity or another whether it was early American intelligence collectors monitoring the newspapers of their rival during the Civil War (CLASS SOURCE) or what is now today the Open Source Center managed by The Office of the Director of National Intelligence. OSINT collection and analysis has increased over the years as communications networks such as the internet have increased in size and breadth. However the rate of growth has not been mutual in quantity or quality. A few particular ventures primarily in the commercial community have begun to invest in the possibilities of datamining and analyzing open source social networking and media sites for potentially useful intelligence.

It is not uncommon for people to Google their own names to see what comes up on the open internet. There are even particular alerts that one can set up to email them daily with all results from news or the general world wide web that a particular query presented. For social networking sites things can get trickier as most or closed networks with at best a limited preview of search results within their respective part of the 'deep web'. One particular tool, available at socialmention.com will actually focus in on particular social media sites and search for your key terms, and if one so chooses, will send you a weekly list of results. Drawing from this concept the aforementioned professional ventures perform a very similar task yet at a professional grade level.

One such service is attensity.com, which performs additional analysis of the collected data results from the requested search terms, though attensity.com is only one several available services. Visible Technologies, which is a software firm that focuses on social media monitoring, was reported to have been receiving investments from In-Q-Tel, the "investment arm of the CIA" and overall intelligence community. Visible explores more than half a million web sites a day, collecting particular client queries from the likes of "blogs, online forums, Flickr, YouTube, Twitter and Amazon". In the following photograph you can see an example of the graphical user interface for one of Visible's applications. This technology is expected to be utilized in pilot programs for the CIA, as they are currently an end customer of Visible, further government contracts have begun to flow in also. There are plans to broaden the linguistic capacity of the applications so foreign media can be monitored automatically (Shachtman).



Topics: 16 Topics Selected
Date Range: Last 6 Months
Countries: 17 Countries Selected

Welcome to TruVoice®

For the current six months, TruVoice® has collected 511 new posts, of which 65% were neutral. Your sentiment for the current six months is 35% positive.

How do people feel?

How much are people talking?

Who's talking the most?

1	Benn	+ New
2	Troy Vogel	+ New
3	STRONGBAD007	+ New
4	ajb62787	+ New
5	pukara99	+ New
6	Roxer	+ New
7	???????????? prolink	+ New
8	Hondaguy900	+ New
9	admin	+ New
10	Adrian Kingsley-Hughes	+ New

more on authors

Where are people talking?

1	secondcitizen.com	+ New
2	blogspot.com	↓
3	phillyblog.com	+ New
4	livejournal.com	↓
5	nintendo.com	+ New
6	feedburner.com	↑
7	testmy.net	+ New
8	xpbanter.com	+ New
9	hostingforum.ca	+ New
10	urbanplanet.org	+ New

more on domains

Marketing Dashboards
View detailed marketing data values and trends from Country, Post, Author, and Domain perspectives

Topic Summary
Take a closer look at how people feel about your topics, and how much they are saying

Data Dashboard
Use the Data page to quickly find the posts at the heart of these dashboards

EcoSystem
Explore the relationships between sites and authors to understand who's talking and where

Last Data Refresh was on Sep 04 at 04:07pm

Another crucial factor in the need for the intelligence community to increase its awareness, use, mirroring and collection of open source resources is that our adversaries are increasing their use of open source channels. In 2008 a US Army Intelligence report was published from the 304th Military Intelligence Battalion based out of Fort Huachuca, Arizona. Ft. Huachuca is the Military Intelligence school for basically all the services' intelligence occupations. The report was posted on the Federation of the American Scientists internet site. The report details the potential uses of modern technology that is available to the public such as mobile phone applications for "digital maps, GPS locators, photo swappers, and Twitter mash-ups of it all." The report showed that Al Qaeda connected internet forums had guidance on how to use specific GPS enabled cell phones for the purposes of land navigation and weapons marksmanship amongst other needed skill sets for conducting terrorist operations. Further guidance was also discovered on how to use voice modification applications and cell phone cameras for conducting ISR operations against their targets (Shactman, 4).

The report also detailed a number of possible uses that the Twitter application could be utilized for instant real-time communications between terrorist operators, much how Twitter and other social networking sites were used by activists at the Republican National Convention and in Iran during the heated elections of 2009. The report however did admit that there were no known occurrences of this by terrorists, however were sure to mention the existence of pro-Hezbollah Tweets. Furthermore the report annotated a possible scenario where terrorists could use social networking sites like Twitter to elicit sensitive information from government employees, and more specifically American soldiers (Shactman, 4).

It is also not surprising that terrorists and their sympathizers use various online social forums such as chat rooms, bulletin boards and blogs (Shactman 7). There are even civilian citizens who peruse and search these social internet areas and attempt to vet out anyone claiming to be a terrorist, to then report them to the authorities. The intelligence community needs to be sure it has a full grasp on this channel of communication for the purposes of monitoring the communication in order to collect on the suspects and also from a counterintelligence standpoint; many plot spoilers could be implemented (shactman 6). One recent real world example of terrorist use of social networks is Umar Farouk who attempted to detonate an explosive device on a Chicago bound flight in December of 2009. It has been reported that Farouk used these open source forums for seeking religious advice (tmcnet).

There is another potential threat that exists, which in 2008 elicited a presentation at the Director of National Intelligence Open Source Conference to detail the possibilities. There has been some talk in the counterterrorism and intelligence communities about the possibility that terrorists could potentially utilize virtual worlds for training, planning and preparation of real world attacks. In this particular presentation it was proposed that terrorists could for example use the online gaming virtual reality of World of Warcraft. The presenter detailed how digital map overlays could be used to conceal a real map of a real target location and that all communication could be done in gaming code-speak (Shactman 8).

With so many open source potential methods of use by terrorists available, it is apparent that the intelligence community for the purposes of counterterrorism need to find their way more involved in collection and monitoring of these open source channels. One open source channel that has been greatly considered a viable utility for terrorist use is Voice Over Internet Protocal or VOIP. The most popular used application is Skype. Skype's particular encryption parameters lend it to being a stellar utility for secure global communications. A terrorist could use Skype from any computer terminal in the world to include many smart phones without the need to have an attributable phone number. Skype also has the ability to transmit instant messaging between Skype users to include the ability to make phone calls and send SMS messages to legitimate phones. File transfers can be conducted also, leaving open the possibility for utilizing steganography as a means to conduct secure data transmission. We must find a way to monitor these types of communications (Skype).

Despite the increase in OSINT operations, there is still a perceivable gap between what we have and what we need. According to one OSINT analyst, there is a slew of issues that riddle the OSINT field. These issues include the following challenges:

1) OSINT is primarily fielded out to contractors who only deal with OSINT as a temporary and preliminary assignment while they wait for their security clearances to process. Once their clearances are granted they are removed from the OSINT field in turn leaving a vital gap, or "brain drain".
2) OSINT analysts do not have access to sensitive databases which leaves them to deconflict datafusion issues, for example discrepancies or similarities in regards to standard naming conventions and identity intelligence. It is easy to track down a hundred John Smiths on Myspace.com, however if their profiles are private there is little one can do to determine the differences between them.
3) Lack of a "shared methodology" for OSINT operations.
4) Lack of counterintelligence standards for OSINT; as most people write off OSINT as less than valuable, when in fact it is the absolute opposite, and its value is increasing as global society becomes more and more connected through open source avenues.

5) The ‘hacker’ community is not reached out to enough for assistance and guidance, despite them being a most valuable commodity and priceless resource tool.
6) Lack in training for OSINT operators. Most operators are out of the perceivable age range that is generally tech-savvy. (Shachtman 3)

In 2007 the Director of the Open Source Center stated to a group of intelligence professionals “we’re looking now at YouTube, which carries some unique and honest-to-goodness intelligence….We have groups looking at what they call ‘citizens media’: people taking pictures with their cell phones and posting them on the internet.” The goldmine of a data cache that is waiting to be sifted through is immense; not only in quantity but also in quality. A former senior technology officer at the Defense Intelligence Agency stated in an email that “Facebook says that more than 70 percent of its users are outside the U.S., in more than 180 countries. There are more than 200 non-U.S., non-English-language microblogging Twitter-clone sites today. If the intelligence community ignored that tsunami of real-time information, we’d call them incompetent” (Shachtman 2).

Despite there being many resources available that remain untapped, the intelligence community is addressing these issues. The intelligence community needs to increase its assimilation and adoption of these open source and social media/network collection resources as it is a large part of the future of intelligence operations and predictive threat management. The new system would incorporate all of these sources as monitoring feeds into its context. This amount of data flow and archived datasets in the respective wikibase will no doubtably require a new concept of data retrieval and renovated analysis methodologies.

Conclusion

It has been said, that before all major catastrophic events in the world, that if one could analyze the full stream of data from around the world, that the events could have been predicted. There is little fact to go on here to validate that claim. However, it is far from inconceivable to say that if an observer analyzed any system leading up to a significant event that occurred that they could predict something about to happen. If a psychologist could study a man who has had four mental breakdowns, surely they would find a pattern in the man's life, leading up to each breakdown. It however would not be until after the breakdown that the psychologist could look back and say 'oh wait, we saw that coming.' It is very possible, that this holds true for a system or a network. That if one were to carefully analyze the events leading up to a system disruption that a pattern develops.

Human beings do it all the time. In relationships they pick up small minute details that are barely noticeable yet they can read them. If they are smart they can tell something is going on or about to occur. Everyone who has been in a relationship has experienced this before. Now just imagine if there was a system that could do this on a global scale. Imagine if a review of data flows could be done in order to predict some drastic event that is about to occur. What if this was limited to terrorist attacks? Intelligence reports come out regularly saying 'something is about to happen'. Ideally this would be the endgame of the system. For it to have enough data, enough learned intelligence and enough capacity to conduct statistical predictive analysis on global events. The use of quantum computing would ideally be applied to this system. Quantum computing has the ability to calculate probabilities and potential outcomes, not just one at a time, but in theory an infinite number of times all at the same time, though within multiple realities if you will (Al-Khalili).

The intelligence community and in particular its components relevant to the world of counterterrorism are on the cusp of a great evolution. What will come of this evolution if the moment is grasped appropriately has been detailed above hypothetically and practically. The innovations in all fields of science will revolutionize the abilities of counterterror intelligence operations to such a degree that they will cease to appear as they have historically. The future of these community operations will find themselves fused together while simultaneously becoming distributed. The capacity to be a pre-emptive force that sees the solutions to problems before they occur will dramatically transform the geosocial landscape to a context that has all hitherto thought to merely science fiction.

Works Cited & Working Notes

The Pentagon’s New Map

Thomas P.M. Barnett

Technopoly – Neil Postman

The Self Aware Universe – Goswan

Consilience – Edward O. Wilson

The Superorganism

Bert Holldobler & Edward O. Wilson

Marlow

Human Terrain Team filling key role

http://www.usf-iraq.com/?option=com_content&task=view&id=14634&Itemid=110

15 october 2007

M. Mitchell Waldrop - Complexity

http://www.wired.com/dangerroom/2007/08/chinas-high-tec/

Danger Room What’s Next in National Security

China’s High-Tech Surveillance State

By Sharon Weinberger ✉

August 14, 2007

Read More http://www.wired.com/dangerroom/2007/08/chinas-high-tec/#ixzz0mRCkbgGs

David Hambling June 3, 2009 Inside the Military’s Secret TerrorTagging

Tech

www-wired-com_dangerroom_2009_06_inside-the-militarys-secret-terror-tag.pdf

Spy Chips Guiding CIA Drone Strikes, Locals Say

http://www.wired.com/dangerroom/2009/06/spy-chips-guiding-cia-drone-strikes-locals-say/

June 1, 2009 Noah Shachtman

Shacter 5 October 24, 2008 Spy Fears: Twitter Terrorists, Cell Phone Jihadists

Noah Shachtman

http://www.wired.com/dangerroom/2008/10/terrorist-cell/

Noah Shachtman

http://www.wired.com/dangerroom/2008/02/youtube-intel/

February 6, 2008

Spies Mine YouTube for Intelligence

Open source quote in this one too

Shactman 6 http://www.wired.com/dangerroom/2007/10/some-of-her-bes/#more

Some of Her Best Friends Are Terrorists

October 23, 2007

Noah Shachtman

Shactman 7

Terrorists Keep Blogs, Too

Noah Shachtman June 25, 2007

http://www.wired.com/dangerroom/2007/06/terrorists-keep/

Shactman 8

http://www.wired.com/dangerroom/2008/09/world-of-warcra/#previouspost

Pentagon Researcher Conjures *Warcraft* Terror Plot

By Noah Shachtman ✉

September 15, 2008

Skype

http://www.skype.com/intl/en/getconnected/

tmcnet

http://blog.tmcnet.com/blog/rich-tehrani/security/terrorist-umar-farouk-abdulmutallab-a-social-networker.html

Hodge

Targeted Killing Lite: Inside the CIA's New Drone Arsenal

By Nathan Hodge

April 26, 2010

http://www.wired.com/dangerroom/2010/04/in-drone-war-cia-opts-for-smaller-less-deadly-weapons/?utm_source=twitterfeed&utm_medium=twitter

Weinberger

http://www.wired.com/dangerroom/2007/07/drones-go-balli/

Sharon Weinberger

Drones Go Ballistic

July 3, 2007

Can Algorithms Find the Best Intelligence Analysts?

Drummond 1

Katie Drummond April 22, 2010

http://www.wired.com/dangerroom/2010/04/can-algorithms-find-the-best-intelligence-analysts/?utm_source=twitterfeed&utm_medium=twitter

Drummond 2

Spytech Agency Wants Software Brains to Connect the Dots

Katie Drummond December 17, 2009

http://www.wired.com/dangerroom/2009/12/spytech-agency-wants-software-brains-to-connect-the-dots/

Albrecht – Scientific American September 2008

Popular Mechanics – January 2010

Von Neumann & Morgenstern “Theory of Games and Economic Behavior”

Emergence – Steven Johnson

Nexus – Mark Buchanan

The Dancing Wu Li Masters – Gary Zukav

The Singularity is Near – Ray Kurzweil