From: "Aaron Barr" <aaron@hbgary.com>
To: "Patrick Ryan" <patrick@bericotechnologies.com>
Sent: Tuesday, November 02, 2010 11:15 AM
Attach: H&W Analysis Proposal v4.docx
Subject: comments

Hey Patrick,

I only sent to you as I made a few comments that I am not sure how some folks will take. I get a read from you that you have pretty thick skin and probably look at proposals similarly so take a look. Any comments take them or leave them and anything I write feel free to modify. I have no pride in ownership, just focused on a tight proposal with concise messaging. Let me know if you need anything else. I took a stab at a few words for the conclusion, again feel free to do whatever with the input.

Aaron Barr
CEO
HBGary Federal, LLC
719.510.8478

Corporate Information Reconnaissance Cell
November 4, 2010

BERICO TECHNOLOGIES™
BE SMARTER. BE FASTER.

Berico Technologies, LLC
1501 Lee Highway, Suite 303
Arlington, VA 22209
Phone: (703) 224-8300
Attn: Patrick Ryan
Deputy Director, Analysis
pryan@bericotech.com
Veteran Owned Small Business (VOSB)

HBGary Federal

HBGary Federal, LLC.
3604 Fair Oaks Blvd, Suite 250
Sacramento, CA
Phone: 301-652-8885 x117
Attn: Aaron Barr
Chief Executive Officer
aaron@hbgary.com

Palantir

Palantir Technologies
Street
Palo Alto, CA
Phone:
Attn: Doug Phillippone
Title
dougp@palantir.com

Submitted to:
Hunton and Williams, LLP
1900 K Street, NW
Washington, DC 20006-1109
Attn: Mr. John Woods, Esq.
Partner
Phone: (202) 955-1500
Fax: (202) 778-2201
jwoods@hunton.com

Background

Internet based communications, most predominately ~~now~~ the growing spectrum of social media platforms, allow people to coordinate and communicate in a highly efficient and collaborative manner, even when highly geographically distributed. These same services and technologies can also make it difficult to attribute information to specific entities. Anonymous and mis-attributable technologies used to mask location and identity have become commonplace. In many cases, people and/or organizations use the inherent insecurity in Internet communications to conduct criminal or morally questionable activities. This represents a paradigm shift in the capability of individuals and small groups to conduct effective planning and execution of asymmetric operations and campaigns that can have major impacts on large organizations or corporations.

Despite the increased capability and anonymity that these technologies provide, it is still possible to counter individuals and groups who are leveraging them to conduct criminal activities. In these cases, it is necessary to develop a more forward leaning investigative capability to collect, analyze, and identify people or organizations conducting such activities. In order to effectively track and understand the complex, interconnected networks involved in these actions, it becomes critical to utilize the latest, cutting-edge tools and analytical processes; applying them in a deliberate, iterative manner against those involved in illicit activities. The best way to limit the capability of these groups is to develop a comprehensive picture of the entities involved through focused collection, conduct rapid analysis to identify key nodes within the network, and determine the most effective method for influencing/limiting these entities.

Developing such a capability requires expertise in:

- Threat Intelligence
- Social Media Exploitation
- Influence Operations
- Traditional Exploit Development
- Open Source Analysis
- Digital Forensics and Malware Analysis
- Network Incident Response
- All-Source Intelligence Fusion
- Targeting/Intelligence Cycle
- Intelligence, Surveillance, and Reconnaissance (ISR)
- Data Integration (Oracle, SQL)
- Custom Software Development

Team Themis

Built around several leading companies who are trusted within the Intelligence Community (IC), Team Themis provides the agility and commitment to the mission and a dynamically efficient approach that delivers tangible results. Our team provides the following strengths:

- Years of experience conducting Information Operations campaigns; successfully managing Intelligence, Reconnaissance, and Surveillance (ISR) lifecycles.
- Cutting-edge collection and analytic technologies and methodologies to provide thorough information intelligence on individuals and groups of interest.
- Complete expertise in all areas of the ISR Lifecycle.
- My 2 cents the previous bullets feel overly BD'ish in that they don't really say much, mostly high level mother and apple pie statements.

□ ~~*Fresh perspectives in the Information Age* from companies that progressively apply lessons learned to support operations and determine internal research and development (R&D) investments.~~

□ ~~*Operational presence across organizations* that harness current applications to provide a *low-cost investment* to deliver capability for all users.~~

- ~~*Strategic impact to the capabilities of the organizations* by leveraging the latest commercial and government technologies.~~

Team Themis is ideally suited to provide Hunton & Williams LLP this critical capability, delivering an innovative and highly effective solution grounded in a deep understanding of the problem set and extensive experience in providing game-changing results across the Intelligence Community and defense/government sector. Team Themis is poised to apply our knowledge and skills to provide Hunton & Williams LLP rapid, effective results that impact the organization's operations and support clients across the space.

Palantir Technologies
Company Background

Berico Technologies

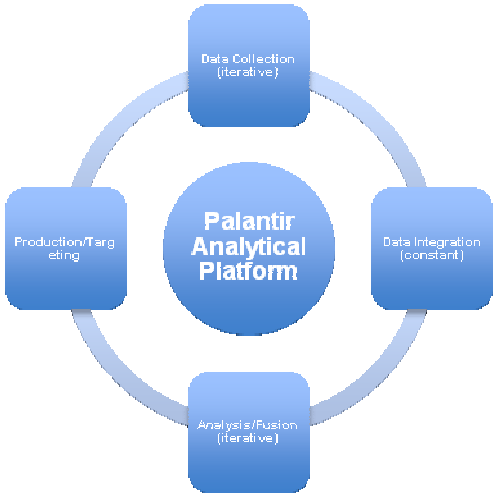
I took out the graphic because the same bullets are already listed in the introduction.

Berico Technologies, LLC is a Veteran Owned Small Business (VOSB) providing analytical and information technology development services to the US intelligence community, Department of Defense and Homeland Security. Berico's mission is to leverage the greatest industry talent in the form of developers, engineers, integrators, and analysts to identify and resolve highly complex national security challenges that require innovative solutions. We offer a full spectrum of services from policy and planning through design, development and delivery directed at improving operational and oversight capabilities, reducing costs and increasing efficiencies. Much of Berico's success results from our unique and respected viewpoint – we understand the battlespace. Through direct support of National, Tactical and Sanctuary organizations, Berico has participated intimately in highly successful projects that have delivered measurable improvements to the warfighter and senior level decision makers around the globe. Berico's unique ability to combine streamlined organizational business processes with operationally relevant experience and technical innovation has earned the company a reputation in the space as a leader and proven difference maker. Our versatile and experienced employees work to ensure that our clients' expectations are met or exceeded.

HBGary Federal
HBGary Federal is an information security services company providing lifecycle support for enterprise incident response, malware analysis, and information operations. HBGary Federal's mission is to provide the best Cyber security and Information Operations specialists, threat and malware analysts to assist our customers in advancing the nations capabilities in securing cyberspace and combating evolving threats. Our focus is bringing together creative, technical talent, experienced threat and intelligence analysts, and mission and cultural experts to develop unconventional and innovative cyber security capabilities. As a core strength HBGary Federal leverages HBGary's incident response and malware reverse engineering and analysis tools, and brings extensive experience in information operations and cyber security at the national level. Specific to this effort HBGary Federal brings extensive experience in the following areas: 1) Influence Operations; 2) Social Media Exploitation; 3)Threat Intelligence and Open Source

Analysis; 4) Vulnerability Research and Exploit Development; 5) Digital Forensics and Malware Analysis; and 6) Incident Response.

Team Themis Solution



New challenges demand new innovative solutions. We propose the creation of a Corporate Information Reconnaissance Cell (CIRC) to provide your organization with a full spectrum capability to collect against, analyze, and affect adversarial entities and networks of interest. Our proposed solution includes the establishment of a robust network architecture (and supporting infrastructure), the identification and collection of all critical data, the seamless integration of this disparate data into a single analytical platform, the stand-up and operation of a team of expert analysts to drive rapid, iterative intelligence cycles, and the production of tailored briefings, reports, assessments, and other analytical products.

Architecture/Organization

Team Themis will establish a comprehensive network architecture that will serve as the foundation for all of the data collection, integration, analysis, and production efforts within the ~~CTAC~~CIRC. Additionally, we will design and build a complementary physical infrastructure and workspace that will enable rapid, continuous analysis in a secure environment.

[insert graphic showing architecture]

-Architecture/hardware requirements (server, computers, monitors, network components)
-Physical infrastructure – working space, power, "fusion cell" mindset
-Other (Furniture, displays, projectors, etc.)

Additionally, Team Themis will work hand-in-hand with the customer to develop a physical and logical layout plan that will facilitate rapid collaboration and analytical discovery. Based on our extensive experience in intelligence analysis and targeting, we believe that the ideal model is the "fusion cell" concept developed and utilized by Joint Special Operations Command (JSOC) elements in partnership with Other Government Agency (OGA) analysis elements. One of the key principles of the fusion cell model is the creation and maintenance of true "situational awareness" among all stakeholders and decision-makers, facilitated by sharing a common workspace and developing multiple methods to visually display user knowledge and analytical findings. This environment is critical to creating a collaborative and functional analytical cell and will be factored into the planning process for layout/construction of the CTAC.

Data Collection

We use a combination of open source tools and data subscriptions combined with custom data collectors and pre-processors. Our methodology for collection is tailored for the social media environment, an iterative process of traditional data collection and social media link and artifact collection and analysis that allows us to make information correlations that would not otherwise be apparent. We use a variety of creative techniques to gain access to information, including the creation of new media content tailored for target audiences. This process allows us to more fully enumerate points of information exposure and identify digital artifacts of interest on individuals and organizations. We complete the first iteration developing organization and individual profiles that dissect each entities digital characteristics and social relationships as they connect back to the overall objectives.

Primary information resources:
1. Background Checks
2. LexisNexis
3. LinkedIn
4. Facebook
5. Twitter
7. Other social media and location services
6. Subject specific sites, blogs, and forums
7. Well crafted search queries to search for digital artifacts
8. Other digital information discovered or given access to during the investigation

The key to successful open source Intelligence, Surveillance, and Reconnaissance is to iterate through the lifecycle quickly and accurately for as complete data collection as possible. Social media encompasses vast amounts of information, much of it potentially ambiguous, so comparative analysis between information sources is key to derive accurate intelligence. We have significant experience in this type of analysis and our methodology has proven out in real operations.

If needed or desired we have the ability to create very realistic web content to engage specific audiences to gather more in-depth information. Sometimes direct target engagement can provide very valuable information that ~~can not~~cannot be acquired through other means. This encompasses persona creation, landing pages, and other development of new media content. For this to be successful it requires a strong understanding of the target as well as a strong understanding of how to use such techniques in operations.

Data Integration
Team Themis developers and engineers will leverage their extensive knowledge of Palantir's development and data integration environments to allow all relevant data to be viewed in one powerful, intuitive analytics layer. All of the data collected will be seamlessly integrated into the Palantir analysis framework to enhance link and artifact analysis. The platform's powerful approach to data integration will allow enterprises to unify data schemas allowing analysts to visualize and query otherwise disparate pieces of information in a secure and collaborative environment. Thanks to Palantir's sophisticated data integration capabilities, analysts within the CTAC will also be able to ingest both structured and unstructured data and perform real-time entity resolution against user-defined criteria on the fly, enabling the fusion of multiple data sources and enrichment of single-source data feeds.

Palantir's open and dynamic ontology capability will provide the flexibility to store and contextualize all types of data for analysis. Team Themis will work closely with the customer to conceptualize and implement a tailored ontology that considers the specific problem set and maps data into human-oriented models to drive effective decision-making grounded in deep understanding. By providing this context and data enrichment, analysts will be empowered to

develop robust link analysis between people, organizations, and other digital artifacts that will begin to form trends and statistical probabilities.

Team Themis will also develop specific helpers to further automate some data ingestion from commercial data sources as well as social media services and Google queries. Team Themis developer/engineers have extensive experience developing against Palantir's open API, allowing us to create customized helpers and applications designed to integrate specific data sources or support common analyst workflows. The development of these tailored applications within the Palantir platform will greatly improve our ability to conduct rapid iterations of the targeting cycle in order to better understand the adversary network(s). In addition, Team Themis has extensive experience in the integration of other existing helpers and tools with Palantir in order to provide capabilities including entity extraction, social network analysis, natural language processing (NLP), custom visualizations, alerting, and thematic mapping.

Analysis/Fusion

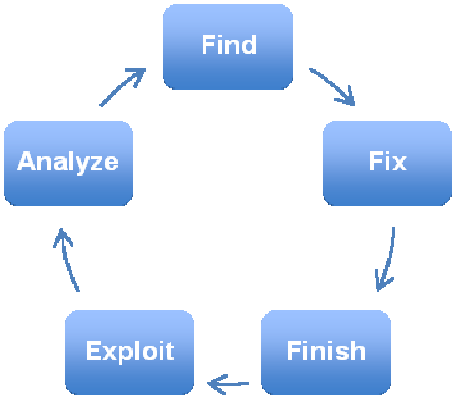
Team Themis will also provide an agile team of intelligence experts trained to leverage the robust capabilities of Palantir to conduct rapid, iterative intelligence/targeting cycles in order to understand and affect identified adversaries. The powerful combination of the Palantir analytical platform and Team Themis collector/analysts will deliver a comprehensive capability allowing Hunton and Williams LLP to truly understand and eliminate emerging threats that could cause harm to their clients.

Leverage the leading analytical platform. Team Themis will utilize the powerful Palantir platform as the centerpiece of the ~~CTAC~~ CIRC – empowering our collector/analysts with a cutting-edge analytical capability that enables rapid search and discovery, effective collaboration, and intuitive knowledge management. Palantir is recognized as the market-leading analytical platform for counter-intelligence (CI), counter-terrorism (CT), counter-narcotics (CN), and counter-proliferation (CP), currently deployed across elements of the intelligence, defense, and law enforcement communities that include SOCOM, DIA, CIA, and JIEDDO. The platform's proven record of success is grounded in the Palantir philosophy of augmenting and empowering analysts with a flexible, intuitive set of tools and capabilities that allow for analysis of data across relational, temporal, and geospatial domains.

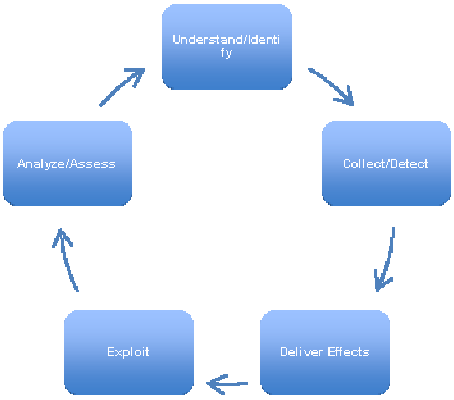
Using the core tools and features in the platform combined with customized helpers and apps (developed by our expert engineers), Team Themis will build a comprehensive picture of threat networks and entities. Through the deliberate application of link analysis and social network analysis (SNA) methodologies, we will gain an understanding of which groups and individuals are working together, what their intentions/plans are, and how to best stop them. Using the real-time, integrated search capability built into Palantir, Team Themis will explore networks conceptually to discover how entities are related and connected as well as set/save search parameters to proactively tip analysts to new information as it becomes available. Additionally, we will utilize the temporal and geospatial functionality within the platform to identify and leverage patterns for predictive analysis, allowing our team to essentially "get inside the decision cycle(s)" of our adversaries. Team Themis will also leverage the collaborative features of the platform to allow our team of collectors and analysts to bring together relevant threat streams and provide fused, multi-INT assessments of relevant entities and adversaries. Finally, we will carefully track and audit our analytical efforts using Palantir's access control model, enabling our team to create and audit trail of who and when made particular changes to objects and their properties. This is particularly important for protecting civil liberties and privacy control.

Apply the most effective analytical processes and methodologies. Team Themis will draw on our extensive operational and intelligence experience to rapidly make sense of the volumes of data we've collected through the application of proven analytical/targeting methodologies. Drawing on the principles and processes developed and refined by JSOC in the *"Find, Fix, Finish,*

Exploit, Analyze" (F3EA) targeting cycle, we will develop and execute a tailored CTAC intelligence cycle suited to enable rapid identification/understanding, refined collection/detection, focused application of effects, exploitation, and analysis/assessment.

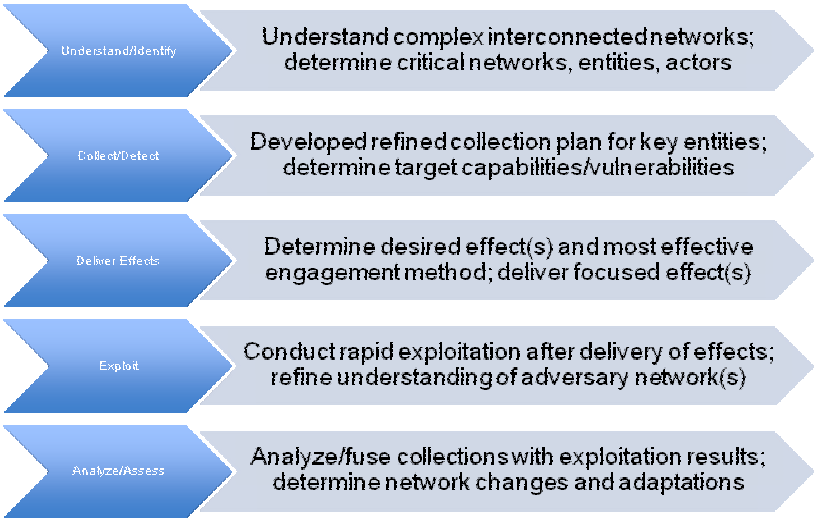


F3EA Targeting Cycle



CTAC Targeting Cycle

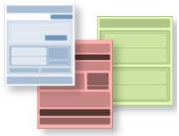
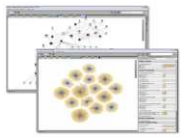
Team Themis will aggressively drive and manage the CTAC targeting cycle to develop a comprehensive threat picture and determine the best method to affect/degrade adversaries based on a nuanced understanding of their capabilities and vulnerabilities. Based on the complex, interconnected nature of the threat environment, we will develop the capability to manage a series of iterative, inter-related targeting cycles against multiple groups and entities in order to achieve enduring effects against networked adversaries. Cycles will move at differing rates and be timed and de-conflicted to maximize impact and limit the adversary's ability to detect or predict our activities. The key phases of the CTAC targeting cycle are:



Production/Targeting

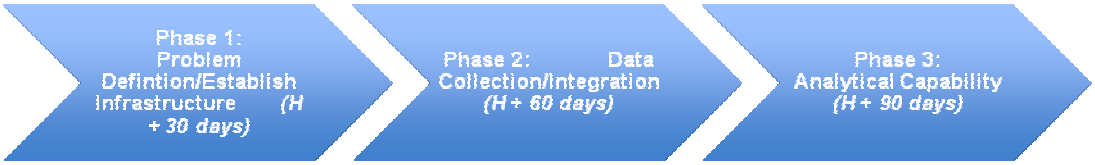
Team Themis will provide full production and planning support throughout the entire targeting cycle in order to ensure that Hunton & Williams LLP has a clear, comprehensive understanding of the intelligence picture. We will work closely with the key leaders and decision-makers from Hunton & Williams to develop production requirements that meet their diverse needs. Given our

experience in all-source analysis and production, we have the ability to produce detailed, customized products, briefs, and reports that will enable situational understanding and (if desired) drive the decision-making process for key leaders within the organization.
Given the unique nature of this problem set, we recommend the following products:

Written Assessments	*Network Visualization*	*Target Folders*	*Targeting Briefs/Meetings*
			
-Daily Intelligence Summary -Weekly Assessment -Special Assessments	-Link Diagrams -Social Network Analysis	-Detailed Dossiers -Pattern of Life -Target Impact Analysis	-Target Lists -Recommended Actions -Network Effects

Timeline

This effort will be conducted in Three Phases:



Phase I – Problem Definition/Establish Infrastructure
-Conduct rapid assessment of problem; determine key tasks and functions; determine infrastructure requirements
-Begin identification of all critical data sources; initial development of custom bots and helpers
-Establish physical location and stand-up staff (including Palantir certification of all analysts)

Phase I is estimated to conclude 30 days following contract award and will require:

1 x Project Manager [Berico]
1 x Forward-Deployed Engineer [Palantir]
2 x Software Engineer [Berico/HBGary]

Phase II – Data Collection/Integration
-Fusion Cell is IOC (all hardware/infrastructure components online)
-Conduct initial collection of critical data sources and ensure seamless integration of persistent data sources
-Develop customized bots and helpers based on analyst feedback and refined mission requirements
-Develop and refine analytical processes and production requirements
-Complete Analyst certification for all members of fusion cell

Phase II is estimated to conclude 30 days following conclusion of Phase I and will require:

1 x Project Manager/Senior Analyst [Berico]
1 x Forward-Deployed Engineer [Palantir]
2 x Software Engineer [Berico/HBGary]

2-3 x Embedded Collector/Analyst [Berico/HBGary]

Phase III – Analytical Capability
-Fusion Cell is FOC
-Continue to aggressively seek out and integrate relevant data sources
-Continue to develop customized bots and helpers as needed
-Conduct iterative targeting cycle(s) based on prioritized requirements from customer
-Conduct regular production requirements (as outlined above)

Phase III represents enduring, steady-state operations and will require:

1 x Senior Analyst/Program Manager [Berico]
½ x Forward-Deployed Engineer [Palantir]
2 x Software Engineer [Berico/HBGary]
3-4 x Embedded Collector/Analyst [Berico/HBGary]

Roles and Key Personnel

Berico Technologies has established an industry high retention rate of 98% for the past three years.

Team Themis places a great deal of emphasis on finding the most talented people, offer them the most competitive compensation and benefits package and employ them on dynamic, high-profile and challenging projects anywhere in the world. The model member of our Team's culture is a consummate student, motivated self-starter and has a passion for solving the toughest problems with the highest quality solutions. Every Team employee is an intelligent, creative and innovative professional who is able to leverage their considerable talents to solve our clients most difficult and high-visibility problems. Team Themis is able to provide our clients with premier service and solutions because of the work ethic and relevant expertise of our employees.

Senior Analyst/Program Manager	-Key duties
Forward Deployed Engineer	-Key duties
Software Engineer	-Key duties
Embedded Collector/Analyst	-Key duties

Guy Filippelli, CEO, Berico Technologies
Guy Filippelli is a former U.S. Army Military Intelligence officer with service in Germany, Korea, Iraq and Afghanistan, and as a civilian Special Assistant to the Director of the NSA. He was recognized as one of four recipients in 2008 of the National Intelligence Medallion from the Director or National Intelligence – the highest award for civilians working within the intelligence community. Mr. Filippelli is a Center for a New American Security (CNAS) Next Generation National Security Leader and an Associate of the West Point Combating Terrorism Center. He most recently returned from several weeks in Afghanistan in June 2010, conducting a comprehensive assessment for senior defense and intelligence officials.

Doug Philippone, DOD Lead, Palantir Technologies
Doug Philippone leads the Department of Defense program for Palantir Technologies Inc. Prior to Palantir, Doug deployed to Afghanistan, Iraq and Pakistan for a total of 6 deployments from 2003-2007. He commanded multiple Joint Special Operations Command outstations in support of the global war on terror. Doug ran the foreign fighter campaign on the Syrian border in 2005 to stop the flow of suicide bombers into Baghdad and helped to ensure a successful Iraqi election. As a commander, Doug ran the entire intelligence cycle: identified high-level terrorists, planned missions to kill or capture them, led the missions personally, then exploited the intelligence and

evidence gathered on target to defeat broader enemy networks. He collaborated with other agencies, NGO's, local government and law enforcement to ensure that places such as Ramadi, Iraq, turned from one of the most dangerous areas in the country to an example of progress. Doug also rebuilt schools, helped support hospitals and medical aid missions, worked with key tribal and governmental leaders to gain local consensus, and help move Iraq to self government. Doug was awarded three bronze stars with two valor awards, the joint commendation medal with valor award, as well as many other commendations for his service to the nation. Doug earned a Bachelor of Science degree in Mathematics from the United States Military Academy at West Point, where he also served as class president for two years, and received his Masters Degree in Terrorism Operations and Finance from the Naval Post Graduate School. In his personal time, Doug is also a State Champion competitive cyclist.

Aaron Barr, CEO, HBGary Federal
Previously, Aaron Barr served as the Director of Technology for the Cyber security and SIGINT Business Unit within Northrop Grumman's Intelligence Systems Division, and as the Chief Engineer for Northrop Grumman's Cyber Campaign. As Technical Director, he was responsible for developing technical strategies and roadmaps for a $750 million organization as well as managing approximately $20 million in Research and Development projects. Prior to joining Northrop Grumman, Mr. Barr served 12 years in the United States Navy as an enlisted cryptologist, senior signals analyst, software programmer, and system administrator. As a senior signals analyst Mr. Barr deployed with the 22nd Marine Expeditionary Unit in Kosovo to conduct key tactical signals intelligence collection and analysis in support of operation Enduring Freedom. Mr. Barr has pioneered many uses of the Internet and new media for the purposes of conduction broad information operations campaigns for key intelligence customers.

Issues and Assumptions

-

Conclusion

In this new environment dominated by constant communication, interactivity, and pervasive content production, those organizations that build capability to harness this new communications space, developing actionable intelligence from a sea of information will be well positioned to most effectively dominate their market as well as have a new service capability that could be offered to others. In the end those individuals or organizations that take advantage of the vulnerabilities created by this new space are themselves more vulnerable to being exposed by their use of it. It's a matter of who has greater capability, and who better to develop a corporate information reconnaissance capability than companies that have been market leaders within the DoD and Intelligence Community.

Tie-up statement.
-Growing power to leverage social media analysis
-List additional decisions that they can make; but we can help them make