Simulation of Cyber Impacts on PMESII-PT Variables

Tony Cerri
TRADOC G-27, OE TSC, DSMS
Ft. Eustis, Virginia
anthony.j.cerri.civ@mail.mil

Neil F. Sleevi
TRADOC G-27, M&S Branch, CGI Federal
Ft. Leavenworth, Kansas
neil.sleevi@cgifederal.com

ABSTRACT

The risk of adversaries using cyber operations to adversely impact the United States and its partners abroad is growing. The importance of commercial cyber infrastructure is increasingly apparent in the day-to-day lives of the world's population. Even small outages can have repercussions that impact not only social, commercial, financial, and utility/energy networks, but also government and military operations that may rely on a commercial information infrastructure. The US Army and Joint Staff have placed confidence in a validated, stochastic, discrete-event simulation called Joint Communication Simulation System (JCSS), which has the capability to simulate adversarial cyber operations. In May 2016, JCSS was used in conjunction with Athena, the Army's award-winning, socio-economic effects model which addresses Political, Military, Economic, Social, Infrastructure, Information, Physical Environment, and Time (PMESII-PT) variables in a notional and futuristic (2025) combined, campaign, near-peer warfighting exercise. The combination of JCSS and Athena provides unique insights to Operational Environment (OE) characterization, risk assessment, synchronization, and course of action development. The lessons learned from red cyber operations during this warfighting exercise confirmed the value of using the two models together.

ABOUT THE AUTHORS

Tony Cerri is the Data Science and Modeling and Simulation Director for the TRADOC G-2. He is responsible for the integration of technologies to facilitate Operational Environment representation. Previous assignments include leading the JS J7's Joint Operating Systems Environment, leading the Experiment Engineering Division for USJFCOM J9 and serving as M&S Branch Chief for USJFCOM J9. Tony is a graduate of the United States Military Academy. He earned master's degrees from Central Michigan University in Administration and from the Florida Institute of Technology in Management. His military awards include the Legion of Merit and the Bronze Star.

Neil F. Sleevi, Colonel, AUS (Ret.), holds a Master of Science Degree in Telecommunications from the University of Colorado and a Master of Strategic Studies from the US Army War College. He provides modeling and analytic support to the Modeling & Simulation Branch of the Data Science, Models, Simulations Directorate, TRADOC G-27. He has completed Operations Research careers in the Army Reserve and Department of Army.

Simulation of Cyber Impacts on PMESII-PT Variables

Tony Cerri
TRADOC G-27, OE TSC, DSMS
Ft. Eustis, Virginia
anthony.j.cerri.civ@mail.mil

Neil F. Sleevi
TRADOC G-27, M&S Branch, CGI Federal
Ft. Leavenworth, Kansas
neil.sleevi@cgifederal.com

BACKGROUND

The concept described here involves the use of a deterministic political, military, economic, social, infrastructure, information, physical environment, and time (PMESII-PT)-related simulation tool called Athena, in conjunction with a stochastic, discrete, event simulation tool called the Joint Communication Simulation System (JCSS), in a futuristic, near-peer, campaign-level warfighting exercise in which adversaries' distributed denial of service (DDoS) and virus attacks were targeted against critical civilian infrastructure in a host partner nation. Employing both of these simulation tools synergistically illuminates how financial, social, and governmental factors can be impacted by disruptive cyber operations in such a way as to impede military operations. The results of the proof-of-principle demonstration address the increased capability to conduct cyber planning and effects for campaign-level, near-peer, warfighting scenario exercises.

OPERATIONAL PROBLEM

The processes described and outlined in Army Regulation 350-2, *Operational Environment and Opposing Force Program*, are designed to provide commanders a realistic training environment within the operational training realm by providing a challenging "sparring partner" (AR 350-2, 1). There exists a need to improve the development of training strategies that describe the tactics, techniques, and procedures (TTP) of threat computer network operations as well as ensure that current cyber defensive and offensive training requirements are addressed. The absence of TTPs designed to provide situational awareness of cyberspace limit a commander's ability to visualize the Operational Environment (OE). Cyberspace is a key component of the OE, and it is imperative that it be integrated and synchronized across all war fighting functions (TRADOC, 2012).

The Army has a documented need to incorporate cyberspace and electronic warfare modeling and simulation (M&S) capabilities into planned training and exercises (CJCS, 2013). Guidance from the current Chairman of the Joint Chiefs of Staff, General Joseph Dunford, requires the Army to "incorporate realistic cyberspace conditions, including robust Opposing Force (OPFOR)/Red Teams into exercises, in order to develop capabilities and TTPs; and incorporate lessons learned from operating in denied or manipulated environments" (CJCS, 2014, 4). Also, the TRADOC G-2 is chartered to validate OEs and OPFOR Order of Battle (OOB) within M&S IAW AR 5-11. While operational and mission variables are all affected by cyberspace or vice-versa, the incorporation of the results for the proof-of-principle described herein will better enable commanders to understand and visualize the impacts of cyber operations across the OE.

Growing Importance of Cyber Operations in the Operational Environment

Cyberspace reaches across geographic and geopolitical boundaries, and is tightly integrated with the operation of critical infrastructures and the conduct of commerce, governance, and national security. As noted in *Chairman of the Joint Chiefs of Staff Notice: CJCS Notice 3500.01—2015-2018 Chairman's Joint Training Guidance* (2013, JP 3-12), cyberspace characteristics include:

- Manmade domain
- Physical, functional, cognitive, logical/virtual, and social
- Programming code and protocols define rules of the domain
- Environment and TTPs that evolve at the speed of code
- Constant presence – All phases of operations
- Unlimited, instantaneous (operational) reach (CJCS, 2013, JP 3-12)

OVERALL ANALYTIC FRAMEWORK AND APPROACH

Framework

The overarching Athena-JCSS employment concept was implemented into a warfighting scenario, which for the first time integrated the results of the high-resolution, discrete-event simulations in conjunction with Athena's computational modeling processes. JCSS supported access, replication, and delivery of cyber effects in an OE-relevant context. The warfighting exercise provided the conditions, circumstances, and influences in which the implementation of cyber effects then shaped the decisions of the warfighting commander. This proof-of-principle is imbedded in a technology-assisted analytic framework. TRADOC G-27 employed this approach as an early foray into experimenting with big data analytics and as a tool to understand and visualize the OE. All three areas of big data analytics were included in the concept, namely, predictive (forecasting) analytics, descriptive analytics (discrete event simulation and data mining), and prescriptive (optimization and simulation) analytics. The analytic results produced insights that improved the understanding of commanders and staffs during the warfighting exercise. The approach provided a richer contextual picture of the impacts of cyber operations, as well as insights into the sensitivity of critical communications and information links in a complex, congested, and competitive operating environment.

As shown in figure 1, the overall framework and methodology employed by the Athena Support Team (AST) for addressing Army operational and institutional challenges in realistic cyber effects training includes fusing and synchronizing three aspects of big data analytics: (1) real-world, open source data, (2) discrete event cyber simulation, and (3) socio-cultural computational modeling. Additional tools and techniques could be integrated in the future.

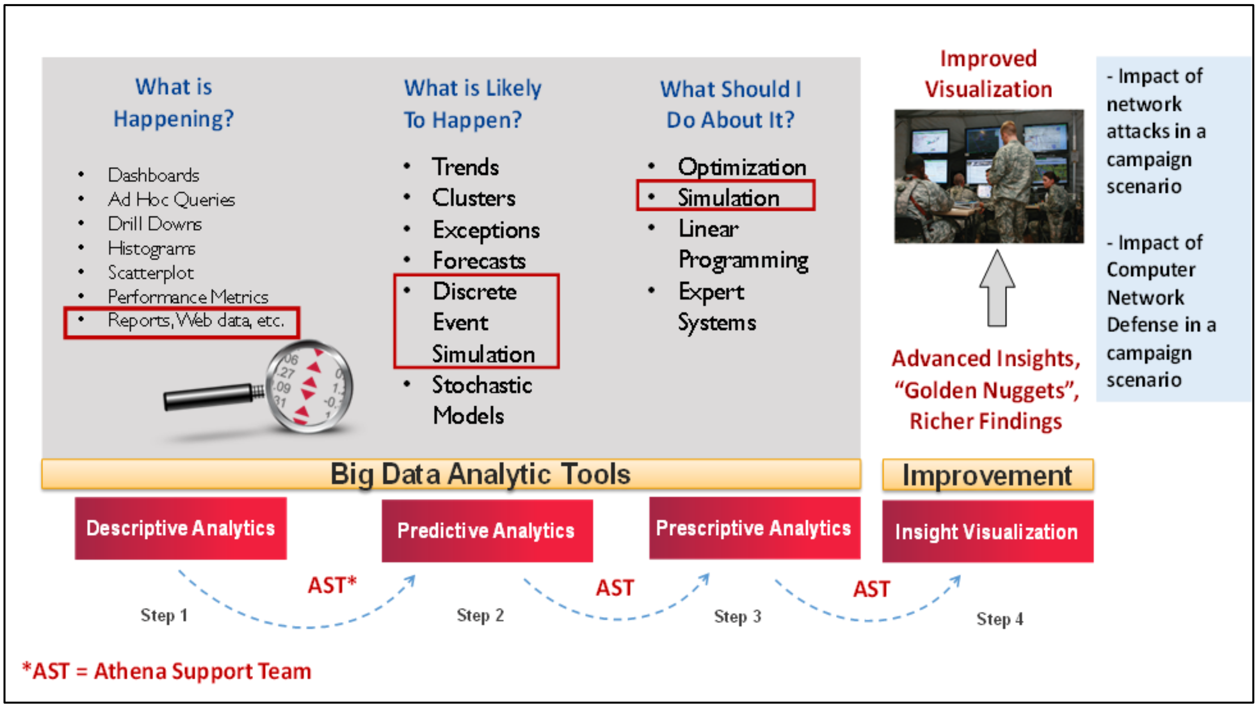
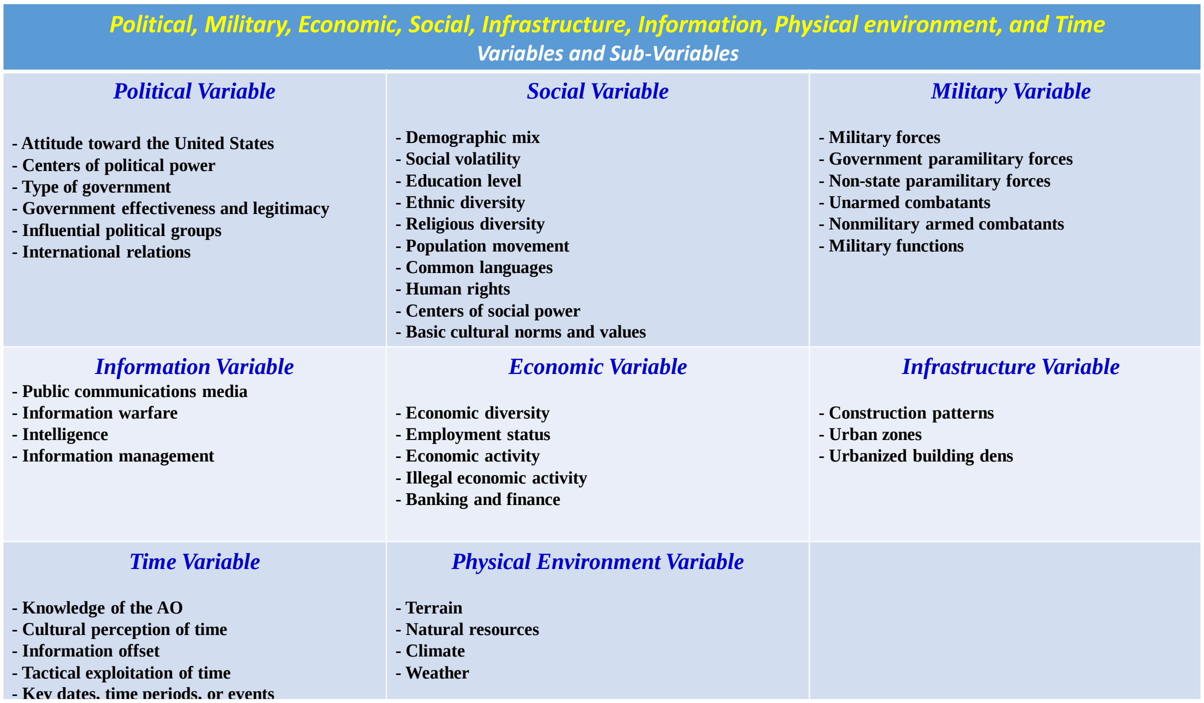


Figure 1: Overall Framework for Cyber Simulation

The AST supported the TRADOC G-2's Threat Emulation Force (TEFOR), which served as the Red Team during the wargame. The JCSS cyber effects model was paired with the Athena Simulation to enable an assessment of the second- and third-order effects of a cyber-attack occurring in a key warfighting scenario. This provided a realistic means to emulate cyber effects upon the PMESII-PT variables. This effort also included determining whether this approach might provide improved understanding of the Army's operational design methodology and the military decision-making process (MDMP). This exercise assessed whether a tool such as JCSS, used in conjunction with Athena, could provide an improved means to evaluate effects on aspects of the OE in order to inform the commander and influence the staff's ability to identify, understand, and predict potential intended and unintended consequences of cyber operations.

Step 1: Descriptive Analytics Used for Characterizing the PMESII-PT Variables

The Athena Support Team conducted historical research into each of the PMESII-PT variables in the scenario area, watching especially for those that might be affected by adversarial cyber operations. These variables and their interrelatedness determine the nature of an OE and how it might affect or be affected by an operation. The OE data sources, include, but are not limited to:



Political, Military, Economic, Social, Infrastructure, Information, Physical environment, and Time
Variables and Sub-Variables

Political Variable - Attitude toward the United States - Centers of political power - Type of government - Government effectiveness and legitimacy - Influential political groups - International relations	*Social Variable* - Demographic mix - Social volatility - Education level - Ethnic diversity - Religious diversity - Population movement - Common languages - Human rights - Centers of social power - Basic cultural norms and values	*Military Variable* - Military forces - Government paramilitary forces - Non-state paramilitary forces - Unarmed combatants - Nonmilitary armed combatants - Military functions
Information Variable - Public communications media - Information warfare - Intelligence - Information management	*Economic Variable* - Economic diversity - Employment status - Economic activity - Illegal economic activity - Banking and finance	*Infrastructure Variable* - Construction patterns - Urban zones - Urbanized building dens
Time Variable - Knowledge of the AO - Cultural perception of time - Information offset - Tactical exploitation of time - Key dates, time periods, or events	*Physical Environment Variable* - Terrain - Natural resources - Climate - Weather	

Figure 2: PMESII-PT Variables and Sub-Variables

- Strategic partners (e.g., NATO, UN, World Bank, international community)
- Interagency partners (e.g., , DoS, DoJ, CIA)
- Multinational partners (e.g., host nation governments)
- Non-governmental organizations (e.g., Doctors Without Borders, USAID) Industry and Academia

Secondary research provided sufficient fidelity for the notional warfighting scenario. PMESII-PT variables and sub-variables were used as inputs to both the JCSS and Athena simulations (see figure 2). Athena was used in Step 1 to calculate initial relationships between and among forces and civilian groups.

The OE represented in this warfighting scenario involved significant deployment of commercial information infrastructure (CII). By 2025, many countries' CII will be increasingly vital to all aspects of PMESII-PT operations. CII for this scenario employed infrastructure in figure 3. CII often includes:

- Voice (including VoIP)
- Data
- Enterprise mobility
- Hosting applications (e.g., Web)
- Data centers

- Cloud computing
- Ethernet, token ring, FDDI, ISDN
- Servers, hubs, switches, modems, routers
- Assumed applications; e.g., YouTube, 8K UHD streaming video and by 2025, “Internet of Things”
- Broadcast TV, radio, Wi-Fi and Wi-Max, satellite TV, etc.

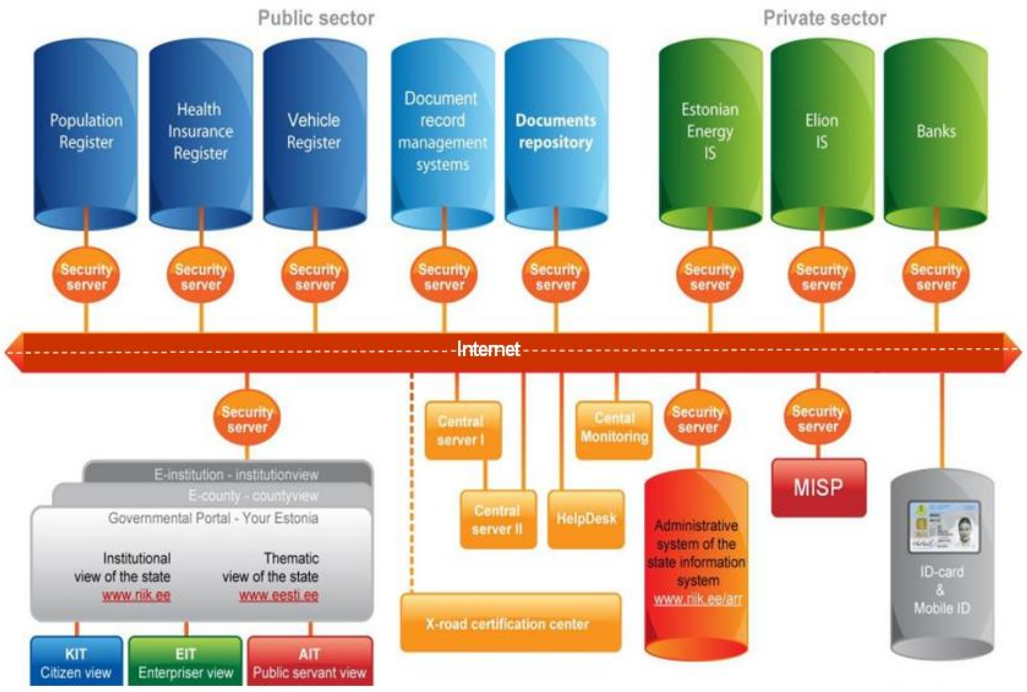


Figure 3. Notional e-Government Commercial System

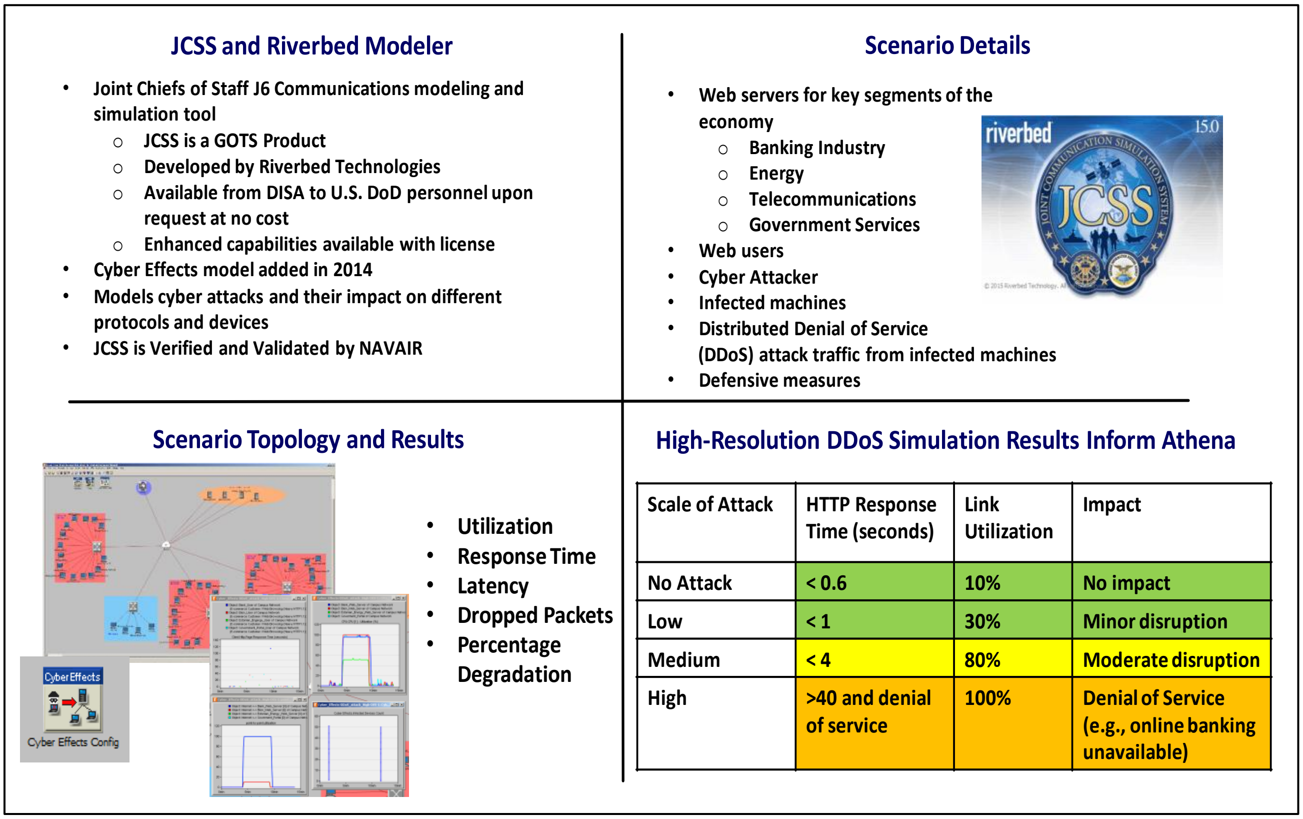
Cyber operations used by Red Forces initially included:

- Distributed denial of service (DDoS) Attacks
- Virus infections
- Cyber sabotage of key infrastructure
- Power grid and SCADA systems
- Backbone network attacks

Cyber operations considered—but not included and may be used in the future—were:

- Confidentiality attacks
- Hacktivism
- Doxing
- Probes and scans
- Integrity attacks
- Malware, etc.

Step 2. Predictive Analytics – High Resolution Simulation with JCSS. JCSS is a Joint Chiefs of Staff-endorsed M&S tool for the warfighter. The software is provided free to DoD civilians, supporting DoD contractors, and military personnel. It has capabilities to simulate cyber effects by providing communications planners and system analysts with the abilities to validate support plans, analyze existing and proposed network architectures, and evaluate the performance of new devices and applications. JCSS offers an integrated ability to analyze communication networks while also providing a validated simulation capability with databases and underlying models so that consistent study results are available throughout the Unified Combatant Commands, Services, and others within the Command, Control, Communications, and Computer Systems (C4) community. JCSS cyber modeling of the OE by JCSS Discrete Event Simulation software provider, Riverbed, allowed high fidelity examination of cyber effects on the commercial information infrastructure, in the OE-see figure 4.



JCSS and Riverbed Modeler

- Joint Chiefs of Staff J6 Communications modeling and simulation tool
  - JCSS is a GOTS Product
  - Developed by Riverbed Technologies
  - Available from DISA to U.S. DoD personnel upon request at no cost
  - Enhanced capabilities available with license
- Cyber Effects model added in 2014
- Models cyber attacks and their impact on different protocols and devices
- JCSS is Verified and Validated by NAVAIR

Scenario Details

- Web servers for key segments of the economy
  - Banking Industry
  - Energy
  - Telecommunications
  - Government Services
- Web users
- Cyber Attacker
- Infected machines
- Distributed Denial of Service (DDoS) attack traffic from infected machines
- Defensive measures

riverbed
15.0
JOINT COMMUNICATION SIMULATION SYSTEM
JCSS
© 2015 Riverbed Technology. All

Scenario Topology and Results

- Utilization
- Response Time
- Latency
- Dropped Packets
- Percentage Degradation

High-Resolution DDoS Simulation Results Inform Athena

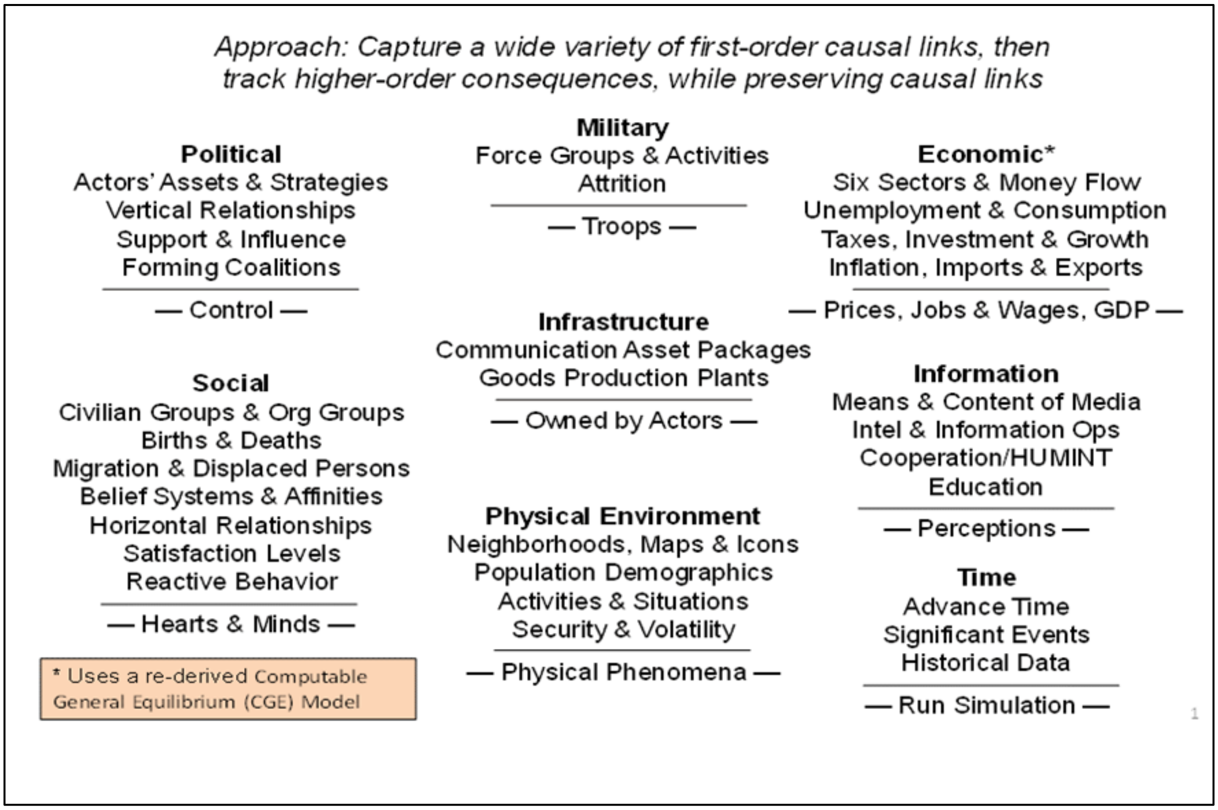
Scale of Attack	HTTP Response Time (seconds)	Link Utilization	Impact
No Attack	< 0.6	10%	No impact
Low	< 1	30%	Minor disruption
Medium	< 4	80%	Moderate disruption
High	>40 and denial of service	100%	Denial of Service (e.g., online banking unavailable)

Figure 4. JCSS Using Warfighting Scenario Predicted Severity of Cyber Attacks on Systems and Users

Step 3. Prescriptive Analytics Using the Athena Simulation (PMESII-PT Modeling) The Athena Simulation shown in figure 5 provided understanding, visualization, and conduct of course of action analyses. Based upon the JCSS results at the warfighting exercise, notional cyber-attack effects were modeled in Athena. The reduction of infrastructure capabilities—in this case, electric power, banking, and telecommunications sectors of the host nation country by its adversaries—was then implemented in Athena.

The effects of these attacks were blamed on the US and its allies through the implementation of a concomitant Information Operations (IO) campaign. Subject matter experts gauged that the disruption of essential services, such as electricity, would have a profound effect on the populace; although, the full impact would be hard to measure as almost all critical infrastructure sectors are connected to the energy sector. Locally affected markets slowed to a halt as commercial utilities and financial institutions struggled to operate with only limited access to the Internet. Frustration with the local government and state legitimacy emerged, resulting in a loss of popular confidence.

The scenario used in Athena was based upon historical cyber-attacks conducted in Europe in the last 10 years. Athena's modeling of the impact of cyber-attacks, as characterized by JCSS, helped Red Force decision makers anticipate the likely consequences, both planned and unplanned, of various threat courses of action. Athena's modeling was comprehensive and anticipated the second- and third-order effects upon competing noncombatant groups and actors as well as potential reactions.



Approach: Capture a wide variety of first-order causal links, then track higher-order consequences, while preserving causal links

Political
Actors' Assets & Strategies
Vertical Relationships
Support & Influence
Forming Coalitions
— Control —

Social
Civilian Groups & Org Groups
Births & Deaths
Migration & Displaced Persons
Belief Systems & Affinities
Horizontal Relationships
Satisfaction Levels
Reactive Behavior
— Hearts & Minds —

* Uses a re-derived Computable General Equilibrium (CGE) Model

Military
Force Groups & Activities
Attrition
— Troops —

Infrastructure
Communication Asset Packages
Goods Production Plants
— Owned by Actors —

Physical Environment
Neighborhoods, Maps & Icons
Population Demographics
Activities & Situations
Security & Volatility
— Physical Phenomena —

Economic*
Six Sectors & Money Flow
Unemployment & Consumption
Taxes, Investment & Growth
Inflation, Imports & Exports
— Prices, Jobs & Wages, GDP —

Information
Means & Content of Media
Intel & Information Ops
Cooperation/HUMINT
Education
— Perceptions —

Time
Advance Time
Significant Events
Historical Data
— Run Simulation —

Figure 5. PMESII-PT Models within Athena

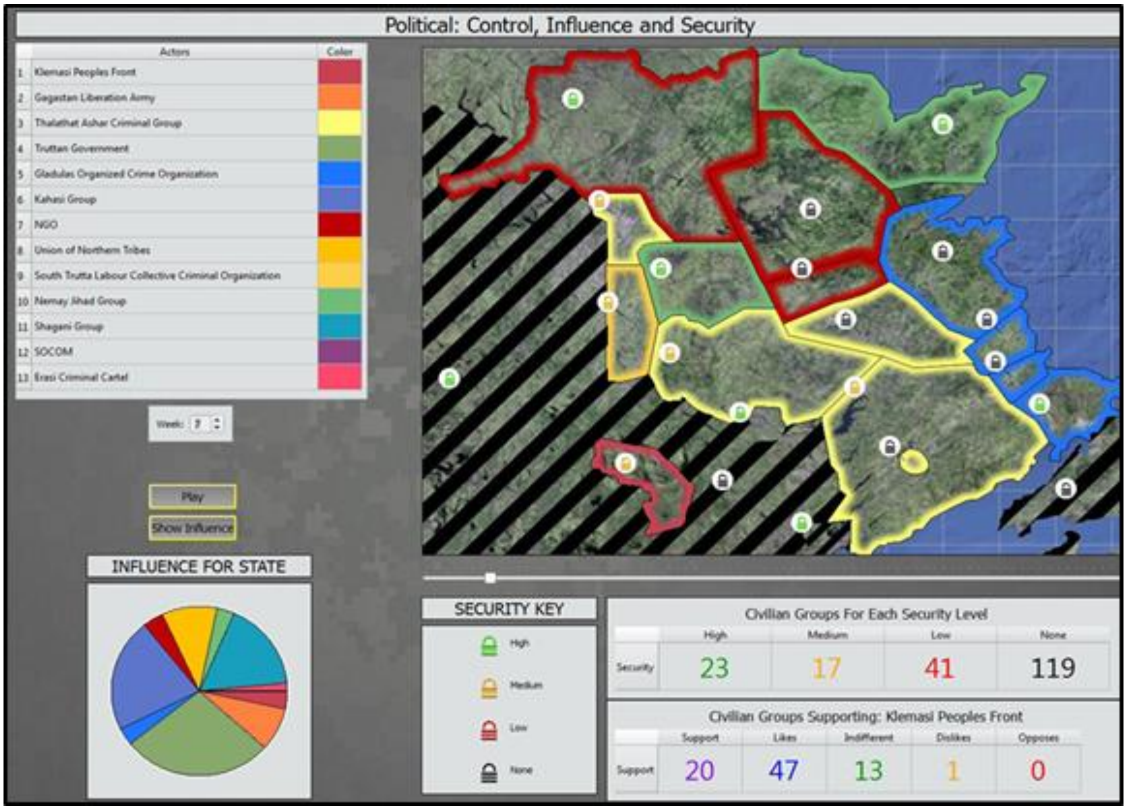
RESULTS

In this notional campaign scenario, the Red Force executed complex and coordinated cyber-attacks in locally contested areas that succeeded in creating problems with banking, transportation, and economic infrastructures. A simultaneous IO campaign by the Red Forces attributed these cyber-attacks to the friendly forces (Blue Forces). In Athena, these tactics resulted in quantitative mood changes among hundreds of thousands of local civilians. The Athena simulation calculates mood (satisfaction) in terms of four factors—namely, quality of life, safety, autonomy, and culture—and found that in these circumstances there was extreme civilian frustration with their local and national governments.

Economic impacts in local areas were substantial as markets failed due to lack of information processing and transaction capabilities. Complex local cyber-attacks on key infrastructure—in particular, the electric infrastructure (this was a wintertime scenario)—stressed the most loyal civilian group's satisfaction with their elected officials. Eventually, the local brownouts and limited flow of goods and services led to the formation of refugee populations which clogged roads and significantly slowed the Blue Forces' freedom of movement. The results demonstrated that the Red Forces had successfully used cyber-attacks not only to delay their enemies and buy time to assess the Blue Forces' intent and objectives, but also to make way for additional Red Force personnel and materiel. Cyber-attacks by Red Forces also led to decreasing popular support and confidence in their local government. Further, the beleaguered host nation government eventually lost enough influence for Athena to calculate a control change in the favor of the Red Forces.

The following describes the Athena impact based on each of the elements of PMESII-PT.

- Political: Cyber-attacks against "soft" commercial infrastructure attributed to Blue Forces reduced political leaders' popular support. Cyber-attacks included: destroying, disrupting, or taking control of targets; protests and retaliatory actions; espionage. Actor control changes are depicted notionally in figure 6.



	Actors	Color
1	Klemasi Peoples Front	🟥
2	Gagastan Liberation Army	🟧
3	Thalathat Ashar Criminal Group	🟨
4	Truttan Government	🟩
5	Gladulas Organized Crime Organization	🟦
6	Kahasi Group	🟦
7	NGO	🟥
8	Union of Northern Tribes	🟧
9	South Trutta Labour Collective Criminal Organization	🟨
10	Nemay Jihad Group	🟩
11	Shagani Group	🟦
12	SOCOM	🟪
13	Erasi Criminal Cartel	🟥

Civilian Groups For Each Security Level

	High	Medium	Low	None
Security	23	17	41	119

Civilian Groups Supporting: Klemasi Peoples Front

	Support	Likes	Indifferent	Dislikes	Opposes
Support	20	47	13	1	0

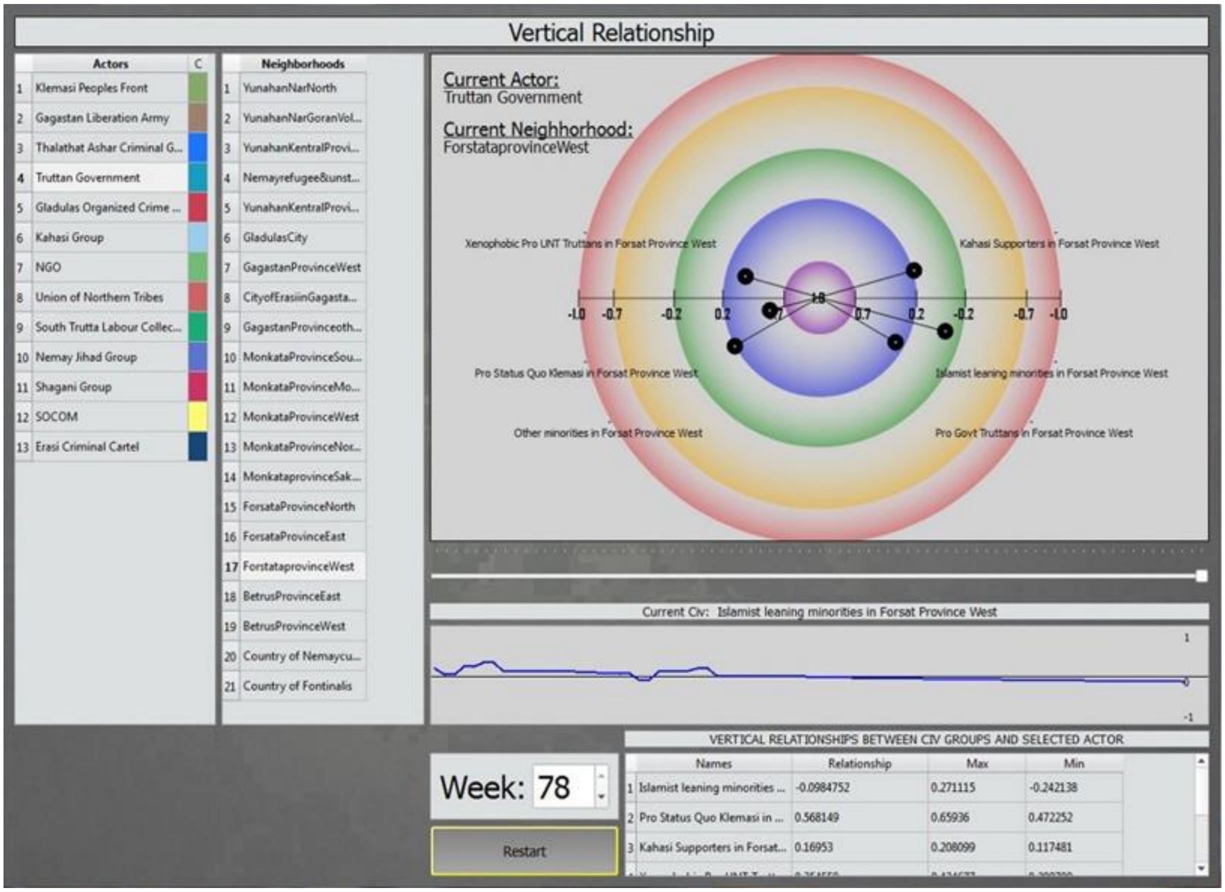
Figure 6. Notional Results: Changes in Influence

- Military: Cyber-attacks slowed the momentum of Blue Forces and allowed time for reinforcement of Red Forces.

- Economic: Cyber-attacks impacted individual and group behaviors related to producing, distributing, and consuming resources. As simulated in JCSS, the Red Forces used a sophisticated "botnet" attack such as was launched in 2007 upon the Estonian Government and commercial websites causing a DDoS. A significant host of computers worldwide were used to conduct that attack, resulting in the complete shutdown of the cyber infrastructure. The Estonian government blamed Russian hackers for this attack; however, the Russian government denied involvement (Gandhi, 2012).

- Social: Cyber-attacks against the commercial economy and infrastructure led to Red Force reduction in all the local civilian groups as well as affected several areas of satisfaction, but most importantly feelings of quality of life and safety. These actions strained and adversely affected relationships between civilian groups and actors. This is notionally shown in figure 7.
  Information: Cyber-attacks affected e-Government and commercial systems that collect, process, disseminate, and/or act on information. This included all Internet-based media and radio/TV. Cyber-attacks were carried out to enable the use of cyberspace to spread propaganda, attack websites, and steal money to fund activities or to plan and coordinate physical-world crime (Gandhi, 2012). Each of these events were modeled in Athena. The future OE will be even more wired to cyberspace and further sensitized to its content; adversary messaging may need to be analyzed and countered in near-real time. As a hypothetical example, if adversary messaging attributed civilian casualties to host-nation or Army forces, imagery and eyewitness documentation (or refutation) of these incidents might be needed within minutes to forestall the formation of flash mobs by otherwise uninvolved civilians (TRADOC, 2012).

- <u>Infrastructure:</u> Cyber-attacks affected the composition of basic facilities, services, and installations needed for the effective functioning of a community or society. Local populations will be reliant by 2025 on an "Internet of Things" environment for all aspects logistics systems, along with civilian financial and infrastructure networks, of transportation, media, banking, and day-to-day economic activity. "Critical military communications and are now dependent on their supporting information systems, leaving them more exposed to crippling cyberattacks" (TRADOC, 2012, 49). Consequences along the dimensions of financial, information, and physical losses are all the more tangible because of a cyberattack. Physical loss in most instances occurs when the cyber world is tightly integrated with the physical world, as in the case of systems that control the distribution of power, gas, water, sewage, oil, and other critical services.



Vertical Relationship

	Actors	C
1	Klemasi Peoples Front	🟩
2	Gagastan Liberation Army	🟫
3	Thalathat Ashar Criminal G...	🟦
4	Truttan Government	🟦
5	Gladulas Organized Crime ...	🟥
6	Kahasi Group	🟦
7	NGO	🟩
8	Union of Northern Tribes	🟥
9	South Trutta Labour Collec...	🟩
10	Nemay Jihad Group	🟦
11	Shagani Group	🟥
12	SOCOM	🟨
13	Erasi Criminal Cartel	🟦

	Neighborhoods
1	YunahanNarNorth
2	YunahanNarGoranVol...
3	YunahanKentralProvi...
4	Nemayrefugee&unst...
5	YunahanKentralProvi...
6	GladulasCity
7	GagastanProvinceWest
8	CityofErasiinGagasta...
9	GagastanProvinceoth...
10	MonkataProvinceSou...
11	MonkataProvinceMo...
12	MonkataProvinceWest
13	MonkataProvinceNor...
14	MonkataprovinceSak...
15	ForsataProvinceNorth
16	ForsataProvinceEast
17	ForstataprovinceWest
18	BetrusProvinceEast
19	BetrusProvinceWest
20	Country of Nemaycu...
21	Country of Fontinalis

Current Actor:
Truttan Government

Current Neighhorhood:
ForstataprovinceWest

Xenophobic Pro UNT Truttans in Forsat Province West
Kahasi Supporters in Forsat Province West
-1.0
-0.7
-0.2
0.2
0.7
1.0
0.7
0.2
-0.2
-0.7
-1.0
Pro Status Quo Klemasi in Forsat Province West
Islamist leaning minorities in Forsat Province West
Other minorities in Forsat Province West
Pro Govt Truttans in Forsat Province West

Current Civ: Islamist leaning minorities in Forsat Province West

Week: 78

VERTICAL RELATIONSHIPS BETWEEN CIV GROUPS AND SELECTED ACTOR

	Names	Relationship	Max	Min
1	Islamist leaning minorities ...	-0.0984752	0.271115	-0.242138
2	Pro Status Quo Klemasi in ...	0.568149	0.65936	0.472252
3	Kahasi Supporters in Forsat...	0.16953	0.208099	0.117481

Figure 7. Notional Results: Changes in Relationships

- <u>Physical Environment</u>: Cyber-attacks during winter weather conditions in this area of operations favored Red operations.

- <u>Time</u>: Cyber-attacks against civilian infrastructure as calculated in Athena and subsequently attributed to the Blue Forces caused significant discontent and refugee flows, which provided the Red Force time to assess Blue actions and reinforce themselves.

DISCUSSION

The integration of descriptive, predictive, and prescriptive analytics in a big data analytics approach coupled with insight visualization tools provided a significant value-added for the TEFOR (Red Forces). This use of JCSS together with Athena may carry forward into future Army Warfighting Assessments. It offered the US military a new means for looking at cyberspace operations effects across the PMESII-PT variables in a future scenario, and it facilitated an improved understanding, visualization, and insight into cyberspace operations and their impact on:

- Red Force TTPs
- Blue Force TTPs
- Country/region/operational domain data
- Access to cyberspace operations best practices and lessons learned

The JCSS cyber effects model, when paired with the Athena simulation, enables important new insights when assessing of the second- and third-order PMESII-PT effects of cyber operations.

SUMMARY AND CONCLUSION

The authors have described an initial approach toward using descriptive, predictive, and prescriptive analytics for improving Army operational design and MDMP assessment and planning processes. The Athena simulation, when used in conjunction with Defense Information Systems Agency's (DISA) validated discrete event simulation, JCSS, allows cyber impacts on CII. Using JCSS and Athena in this way, this undertaking:

- Highlighted the PMESII-PT effects (both offensive and defensive) of cyber operations and allowed staff officers to make informed decisions to maximize their effectiveness in a combined, campaign, near-peer, warfighting, exercise scenario outcome.
- Provided a prototype of the cyber simulation design. Metrics included the system being able to simulate for a training audience a variety of possible cyber-attacks (e.g., DDoS attacks, viruses, hacking, etc.) and added realistic effects to benefit a warfighting and training audience, so they can better determine the nature of the attack and react as appropriate.
- Provided the G-27 M&S Branch an opportunity to test a precursor to big data analytics for OE visualization, understanding, and advanced insights.
- Combined descriptive, predictive, and prescriptive analytics in such a way to provide a richer contextual understanding of the OE.
- Provided an innovative combination and fusing of data by the JCSS and Athena simulations, which increased the ability to understand the intended and unintended consequences of cyberspace interventions. (Note: The results of this effort may lead to enhancements which can be synchronized with ongoing analytic requirements for potential integration into current and future Army Mission Command Systems).
- Provided a viable candidate capable of filling several identified gaps with regard to modeling human domain and cyber operations.
- Showed the utility of integrating results of a stochastic model to provide a second layer of analysis. This may be applicable to other areas such as population follow models, etc.
- Addressed potential Essential Elements of Analysis (EEA) related to future OE interventions. For example:
    - How can the Army improve cyber security operations within the context of a future 2025 combined campaign near-peer warfighting exercise?
    - What is the optimal way in a major future 2025 Scenario to employ cyber capabilities with the elements of traditional combat power to support Unified Land Operations (ULO) and deliver the PMESII-PT effects required by commanders at all echelons?

ACKNOWLEDGEMENTS

The authors are gratefully indebted to the TRADOC G-2 TEFOR—particularly the Director, Mr. Darrell Combs—for continued collaboration with TRADOC G-27 to get the Athena Support Team involved in the exercise in spite of uphill constraints. Likewise Global Cultural Knowledge Network Director, Ms. Penny Mellies' effort was value-added and went beyond normal coordination internal to the OE Enterprise (OEE). Special thanks to Dr. Robert Arp as well, for his research for the scenarios used during this exercise and his document review.

The authors also acknowledge Mr. Steven Crum, DISA, and the entire Riverbed team for assistance with training, supplying a demonstration license for JCSS, and their support in the scenario build.

REFERENCES

AR 350-2 (Army Regulation 350-2). (2015). *Army Operational Environment and Opposing Force Program*. Washington, DC: US Government Printing Office.

CJCS (Chairman of the Joint Chiefs of Staff). (2014). *Chairman of the Joint Chiefs of Staff Notice: CJCS Notice 3500.01—2015-2018 Chairman's Joint Training Guidance*. Washington, DC: US Government Printing Office.

CJCS (Chairman of the Joint Chiefs of Staff). (2013). *Cyberspace Operations. Joint Publication 3-12 (R)*. Washington, DC: US Government Printing Office.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine, 30*, 28-38.

Patel, P. (2016). "Economic Consequences of Cyber Attacks." *Patel's Blog*. Retrieved from http://purvag.com/blog/?p=103

TRADOC (US Army Training and Doctrine Command) G-2 (2012). *Operational Environments to 2028: The Strategic Environment for Unified Land Operations.* Ft. Eustis, VA.