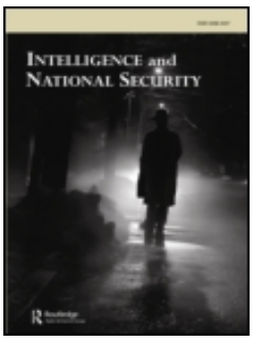

Routledge
Taylor & Francis Group

Intelligence and National Security

ISSN: 0268-4527 (Print) 1743-9019 (Online) Journal homepage: http://www.tandfonline.com/loi/fint20

Probing Uncertainty, Complexity, and Human Agency in Intelligence

Daniel Javorsek II & John G. Schwitz

To cite this article: Daniel Javorsek II & John G. Schwitz (2014) Probing Uncertainty, Complexity, and Human Agency in Intelligence, Intelligence and National Security, 29:5, 639-653, DOI: 10.1080/02684527.2013.834218

To link to this article: http://dx.doi.org/10.1080/02684527.2013.834218

Published online: 13 Dec 2013.

Intelligence and National Security, 2014
Vol. 29, No. 5, 639–653, http://dx.doi.org/10.1080/02684527.2013.834218

Routledge
Taylor & Francis Group

ARTICLE

Probing Uncertainty, Complexity, and Human Agency in Intelligence

DANIEL JAVORSEK II AND JOHN G. SCHWITZ*

ABSTRACT Geopolitical dynamics associated with nuclear proliferation, the Arab Spring, the rapid rise of Chinese power, an oil-fueled Russian resurgence, and the post-Afghan and Iraq eras will demand significant changes in intelligence focus, processes, and resources. Nearly a decade after intelligence failures required a restructuring of the Intelligence Community with mandates for a scientific approach to intelligence analysis, current efforts continue to focus on overly deterministic individual analyst methods. We argue for a process-oriented approach to analysis resembling the collaborative scientific process successful in other professions that is built on shared theory and models. After demonstrating that events in the real world are path dependent and contingent on deterministic and random elements, we highlight the role of uncertainty in intelligence analysis with specific emphasis on intelligence failures. We then describe how human agency in an interconnected and interdependent system leads to a landscape of dancing strategies as agents dynamically modify their responses to events. Unfortunately, the consequences of the present deterministic intelligence mindset are significant time delays in adjusting to emerging adversaries leading to an increased susceptibility to intelligence failures. In contrast with the existing analyst-centric methods, we propose a risk management approach enhanced by outside collaboration on theory and models that embrace lessons from the twentieth-century science of uncertainty, human agency, and complexity.

Science Confronts Uncertainty, Human Agency, and Complexity

Science, its methods and worldview, were radically transformed in the early twentieth century and altered the conventional deterministic interpretations by addressing uncertainty, human agency, and complexity. In 1905, 26-year-old patent clerk, Albert Einstein, published his five *Annus Mirabilis* (from the Latin for 'extraordinary year') physics papers that challenged pre-existing understanding and ushered in a new era of scientific thought.[1] In addition to his revolutionary contributions on special relativity and the equivalence of

*Corresponding author. Email: john.schwitz@gmail.com

[1]John J. Stachel, *Einstein's Miraculous Year: Five Papers That Changed the Face of Physics* (Princeton: Princeton University Press 1998).

mass and energy, his paper on the photoelectric effect introduced the concept of light quantization that contributed to the foundations of quantum mechanics. Coupled with his work on Brownian motion, quantum mechanics would evolve into a theory that upset the previously accepted deterministic view of nature to such a degree that even Einstein himself could not accept the result. In this interpretation, the triad of determinism, reductionism, and stationarity have evolved into a view of a future characterized by probabilities, the observation that the sum of parts produces emergent behavior, and the study of extreme behavior.

The dynamic feedback and non-linear coupled behavior of real world systems has also spurred the more recent development of complexity analysis to a diverse set of conditions and problems.[2] This nascent field blends both the probabilistic physics concepts that took shape at the turn of the twentieth-century with the developing field of game theory.

We emphasize how an overly deterministic intelligence mindset introduces time delays in adjusting to emerging adversaries. Finally, to contrast with the existing hierarchical analyst-centric methods, we propose outside collaboration on theory and models that embrace lessons from the twentieth-century science of uncertainty, game theory, and complexity. Adopting this *community intelligence process* requires increased interaction outside the community, and a shift in the distribution of responsibilities, work, and analytic tools within the Intelligence Community (IC).

The Pull of Determinism in Intelligence

Despite the probabilistic transformation in the natural sciences, economics, and the social sciences, intelligence methods remain limited to the pre-1900 deterministic world view. This is best expressed in the statement made by Marquis Pierre Simon Laplace in 1825:

> We may regard the present state of the universe as the effect of its past and the cause of its future. An intellect … could condense into a single formula the movement of the greatest bodies of the universe and that of the lightest atom; for such an intellect nothing would be uncertain and the future just like the past would be present before its eyes.[3]

One measure of the consensus view on determinism may be found in both the Intelligence Community and the public's qualification of an intelligence failure. The 11 September 2001 Intelligence failure is frequently cited as avoidable if only we could have 'connected the dots'.[4] At the other end of the

[2]Neil Johnson, *Simply Complexity: A Clear Guide to Complexity Theory* (Oxford: Oneworld Publications 2007).

[3]Paul Davies and Niels H Gregersen, *Information and the Nature of Reality: From Physics to Metaphysics* (Cambridge: Cambridge University Press 2010) p.74.

[4]National Commission on Terrorist Attacks, *The 9/11 Commission Report* (NY: W.W. Norton & Company Inc 2004) p.408.

spectrum there are instances where the role of uncertainty in black swan events (high-impact events occurring with low-frequency) are grossly overstated implying a world that is random and beyond our influence. For example, David Viniar, the Goldman Sachs chief financial officer, stated of the 2007 financial crisis: 'We were seeing things that were 25-standard deviation moves, several days in a row'[5] which really should be impossible given the current age of the universe.

Our scientific view maintains that events lie somewhere in the interesting in-between region where human agents can influence loosely coupled causal factors at critical junctures creating an array of possible future events. The future is thus a spectrum of outcomes, each associated with a probability of occurrence.

The first column of Figure 1 represents a common intelligence tool, such as the Analysis of Competing Hypotheses.[6] In this method the analyst frames alternate hypotheses and examines their respective deterministic future outcomes. Unfortunately, even with this approach the pull of determinism is overwhelming, causing the analysts (in the case of National Intelligence Estimates discussed below) to focus on one outcome. In contrast, the second column encompasses the probabilistic nature of future outcomes where each initial condition has a probability of reaching most future outcomes, some of which might be black swans. In fact, in intelligence we rarely fully understand all the factors specifying our adversary's capabilities, motivations, and practice of denial and deception. For example, we certainly do not fully understand the current nuclear capability of Iran but rather rely on conclusions derived from sparse information. This is represented by the cloud of uncertainty surrounding the initial states in column 2.

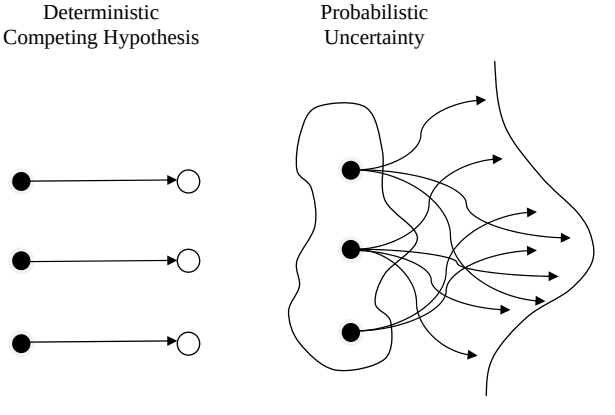

Figure 1. The Contingent Path of History.

[5]Peter T. Larsen, 'Goldman Pays the Price for Being Big', *Financial Times*, 13 August 2007.
[6]Richards J. Heuer and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington, DC: CQ Press 2011) p.147.

Although intelligence poses a more difficult problem, applications of similar probabilistic concepts in the fields of physics, economics, meteorology, biology, and medicine have demonstrated this approach to be robust and adept at representing real-life scenarios.[7]

Why 'So Many' Extreme Events?

First, we analyze the frequency of major intelligence failures over the period 1950–2003 to demonstrate a scientific approach to uncertainty. Since our intent is not to address the often disputed definition of an intelligence failure but rather examine the occurrence of extreme events, following a sampling of the literature we arrived at the consensus of 11 major intelligence failures during this period.

We construct the simplest explanation using Occam's razor, an approach favoring simple over complex explanations. The simplest explanation is that each failure is independent of past failures and the time between failures may be modeled by a statistical process which reflects the expected frequency of events. This is a Poisson process, which is used in a diverse set of real-life problems such as radioactive decay, service demands, machine failures, and warranty repairs. Intelligence failures before 2001 are a reasonable fit to this model with a failure rate of 1.8 failures per 10-year period, equivalent to an average time between failures of 5.3 years.

When observed in this respect, the extreme nature of the 2001 and 2003 intelligence failures (9/11 and Iraq WMD) becomes evident. The failure to predict the 11 September 2001 terrorist attacks, and false attribution of weapons of mass destruction to Iraq, represents a statistically significant increase in the failure rate with a probability of occurrence of less than 5 per cent (the probability associated with two failures in two years is displayed by the large gray square on the solid line of Figure 2). This extreme failure rate compounded by the intelligence communities painfully slow transformation from the cold war provided passionate motivation for reform and provided the tipping point for Congressional intercession in the IC. In its aftermath, several studies of intelligence failures cited a systemic problem in analysis and resulted in the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 which placed the blame squarely on analysis failures within the IC.[8] To quote the WMD Report of 2005:

> The Intelligence Community is at the juncture of a number of powerful historical forces: the end of the cold war, the first catastrophic attacks in the United States by international terrorists, the proliferation of nuclear weapons, the failure of US intelligence in Iraq, the broad-based demand

[7]David Orrell, *The Future of Everything: The Science of Prediction* (NY: Basic Books 2007) p.348.

[8]Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108–458, 108th Cong., (17 December 2004), §1019.

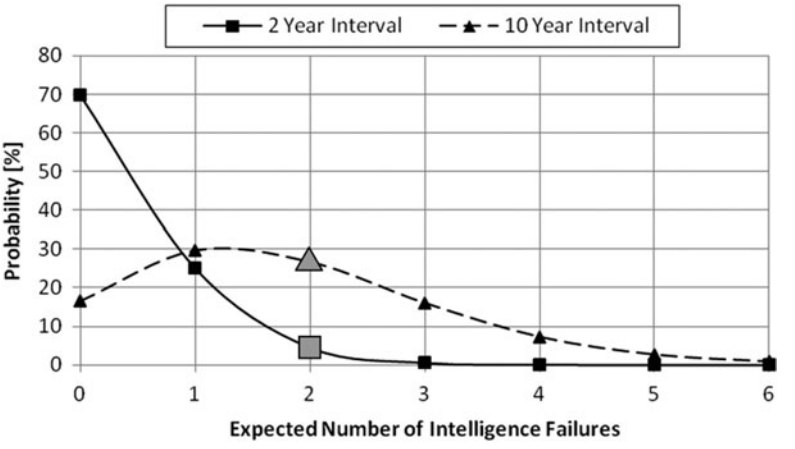

Figure 2. Poisson Probabilities for Expected Number of Intelligence Failures.

> for change by the American people, and enactment by Congress of the most sweeping legislative reform since the creation of the existing Intelligence Community in 1947.[9]

After the Berlin Wall fell in 1989, the rapid dissolution of the Soviet Union in 1991 introduced a geopolitical dynamic the IC failed to adjust to. This is reflected in the WMD report which criticized the IC for a 10-year lag in adjusting intelligence from a cold war focus. However, when the 10-year interval from 2001 to 2011 is considered, the intelligence failure rate remains consistent with historical levels (the probability of two failures in 10 years is 27 per cent and is represented by the large grey triangle on the dashed line of Figure 2) providing support that IRPTA has had an effect.

In fact, eight years after IRPTA we finally have an Intelligence Community that is better adept at countering a terrorist threat than existed before 2001. However, nuclear proliferation, the Arab Spring, the rapid rise of Chinese power, an oil-fueled Russian resurgence, the post-Afghan and Iraq eras, and the resulting budgetary response introduces significant additional risks into the system. This paper addresses recommendations to prevent another 10-year adjustment lag as the Intelligence Community adapts to the next geopolitical environment.

An analysis of outliers (black swan events) often confronts the analyst and policymaker with the reality that they occur at a greater frequency than our traditional analysis and models signal, and that they determine or dominate history. Unfortunately, the Intelligence Community does not capture the basic information on uncertainty to permit an informed statistical analysis on intelligence products. A 2012 publication in *Intelligence and National*

[9]Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (31 March 2005, p.539).

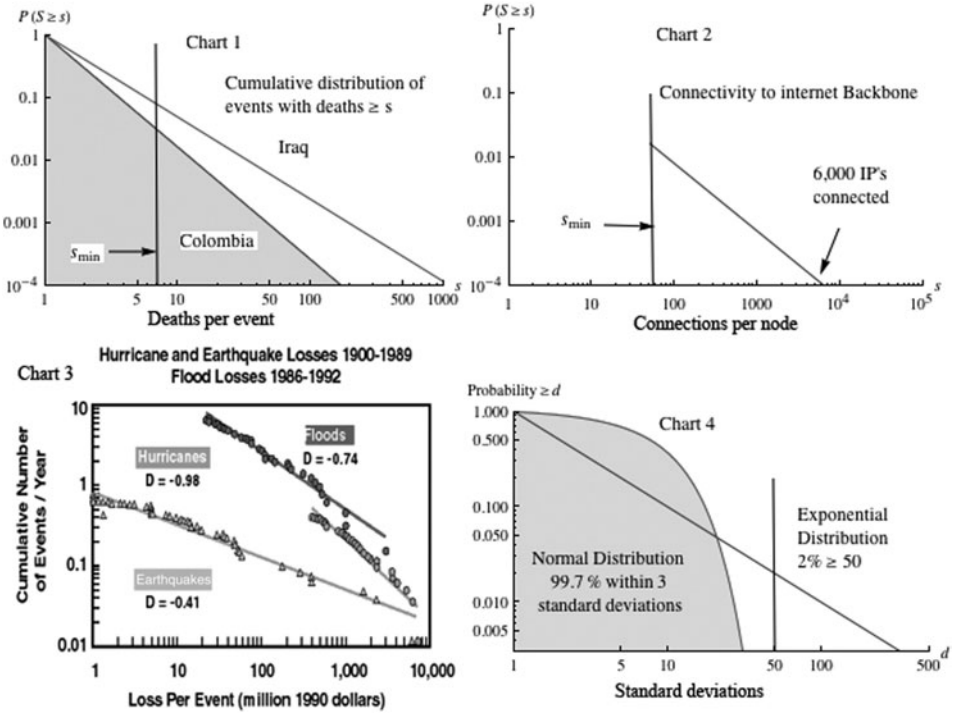

Figure 3. Casualties from Conflicts, Internet Backbone Connectivity, Disasters, and Tail Risk.

Security, 'Assessing Uncertainty in Intelligence',[10] analyzed 379 declassified National Intelligence Estimates (NIEs) written between 1964 and 1994 finding that 53 per cent examine only one possible outcome, 30 per cent examined three or more outcomes, 18 per cent discuss a range of possible outcome, while 30 per cent examine three or more outcomes. From the 379 NIEs, 18 per cent discuss possible outcomes, without giving even a qualitative sense of probabilities, while only 4 per cent use quantifiable probabilities. Only one instance, discussed over two possible outcomes with probability estimates. The study found that the analysis had a tendency to conflate the likelihood of an outcome with the confidence in the intelligence. The likelihood expresses the probability of an occurrence while the confidence qualifies the intelligence by the 'scope, quality, and sourcing' supporting the analysis. Both measures must be independently presented.

These problems are compounded by the extensively discussed short-term focus of intelligence on the Presidents Daily Brief, and the top priorities of the National Intelligence Priorities Framework (NIPF). Our approach of acknowledging and quantifying uncertainty and adding measures of

[10]Jeffrey A. Friedman and Richard Zeckhauser, 'Assessing Uncertainty in Intelligence', *Intelligence and National Security* 27 (5) (2012) pp.8,13 <http://scholar.harvard.edu/files/friedman/files/assessing_uncertainty_in_intelligence_5-21-12.pdf> (accessed 20 September 2013).

significant consequence, discussed later in the paper, shifts the focus to strategic analysis, risk management, and attention to consequences. The evidence from physical processes, that tracking small events signals the probability of catastrophes, indicates that daily intelligence products may serve as a predictor of change and signal the probability of catastrophic events.

Only by explicitly identifying the probabilities of possible outcomes associated with a measure of significant consequence can we evaluate and improve our intelligence process while signaling the probability of catastrophic events. How we do this is presented through examples of the analysis of intelligence and national security concerns presented in Figure 3. The analysis encompasses casualties from terrorism in Colombia and Iraq,[11] the internet backbone,[12] national disasters,[13] and the significance of 'tail risk'.

Complex processes drive this observed behavior, which is radically different from processes generated from distributions with finite variances. The papers referenced develop models to interpret trends and forecast future results. The detailed analytics are beyond the scope of this paper, so a brief summary suffices. Johnson[14] develops models of terrorist behavior, its evolution, and the resulting casualties across a range of conflicts (Chart 1). He also provides forecasting methods and indicators of progress in terrorist conflicts. Yan[15] maps the connectivity of the internet backbone (Chart 2) and discusses the security risks from the highly connected nodes (the arrow points to 6000 IPs at one node). His work uses network analysis, which is also used to study terrorist networks. Link analysis, examining the network connectivity of a terrorist network, is used to discover command and control relationships as well as identify methods of penetrating the network. The US Geological Survey (USGS) captures the frequency and severity of natural disasters[16] (Chart 3), which is used to forecast economic and human losses, and provides the foundation for establishing rates and reserves in insurance. Finally, the extraordinary behavior of exponential distributions on 'black swans' is evident from Chart 4, with further elaboration in Figure 4 which describes the key characteristics of power law distributions.

Extreme events occur at unexpected frequencies in fat-tailed distributions such as the exponential distribution. Accurate identification of the behavior

[11]Neil F. Johnson et al., 'From Old Wars to New Wars and Global Terrorism' <http://xxx.lanl.gov/abs/physics/0506213> (accessed 20 September 2013).

[12]Guanhua Yan, Stephan Eidenbenz, Sunil Thulasidasan, Pallab Datta, and Venkatesh Ramaswamy, 'Criticality Analysis of Internet Infrastructure', *Computer Networks* 54 (2010) pp.1169–82. <http://www.sis.pitt.edu/~dtipper/3350/April_Paper4.pdf> (accessed 20 September 2011).

[13]Natural Disasters – Forecasting Hurricane Occurrence, Economic and Life Losses, USGS <http://coastal.er.usgs.gov/hurricane_forecast/hurr_losses.html>

[14]Neil Johnson et al., 'Dynamic Red Queen Explains Patterns of Fatal Insurgent Attacks', *Science* 333 (2011) pp.81–4.

[15]Yan et al., 'Criticality Analysis', pp.1169–82.

[16]Natural Disasters – Forecasting Hurricane Occurrence.

The Power Law Distribution

Where x measures a significant consequence; the probability of an event x is Probability (x) = $x^{-\alpha}$ over a restricted range of x.

This implies that the graph of log of the cumulative probability against the log of the consequence x is linear with a negative slope of magnitude k = α–1.

$$\log [\text{probability } (X \geq x)] = -k \log [x]$$

The consequence must be expressed in a common numinaire such as dollars, casualties, or network connections.

A Power Law generates self-similar scaling and 'infinite variance'. Self-similarity means, for instance with $\alpha = 2$, that increasing the consequence by a factor of 10x only reduces the probability of occurrence by 1/100thacross the complete range. Observed variances are finite because the relationship applies to a large, but restricted range.

The term fat-tailed distribution derives from the large number of extreme events. This provides a stark contrast to the Normal distribution. A Normal distribution with mean 1 and standard deviation 10 has only 0.3 per cent of the events outside 3 standard deviations (≥ 31). Contrast this with the Power Law ($\alpha = 2$), 3 per cent of the distribution is ≥ 31 and 2 per cent of the distribution is ≥ 50.

Figure 4. Characteristics of a Power Law: Self-Scaling/Infinite Variance.

that exhibits such self-similar scaling *permits the use of frequent small events to more accurately estimate the occurrence of large disastrous events*. Figure 4 describes key characteristics of a power law.

Human Agency: A Difficult Challenge for Intelligence

Game theory formally integrates the element of human agency. It has been used to tackle issues ranging from terrorism[17] to whether current policy decisions will heighten or deter Iran's resolve to obtain nuclear weapons[18] to protecting airports, ports, and air traffic from terrorism.[19] Most famously, game theory was successfully employed to address the continual US/Soviet confrontations during the cold war.

There was never a greater existential threat to the world than the nuclear arms race engendered by the cold war. During the period from 1965–9 the US Arms Control and Disarmament Agency (ACDA) employed a group of

[17]Todd Sandler and Daniel Arce, 'Terrorism & Game Theory', *Simulation & Gaming* 34 (2003) pp.319–37.
[18]Clive Thompson, 'Can Game Theory Predict When Iran Will Get the Bomb?', *The New York Times*, 12 August 2009.
[19]Milind Tambe, *Security and Game Theory Algorithms, Deployed Systems, Lessons Learned* (NY: Cambridge University Press 2012).

10 game theorists who assisted in formulating negotiating strategies for SALT I (Strategic Arms Limitation Treaty), a bilateral armament control negotiation between the USA and the Soviet Union that restrained the number of ballistic missile launchers and resulted in the Anti-Ballistic Missile Treaty.[20] The group produced five technical reports covering decision and game theoretic topics related to arms control.[21] One of the reports in particular (Report 1) addressed the relationship between model building and bargaining pivotal in the development of agent-based modeling that includes human agency. The strategists circumscribed the limits of models and the two-way relationship between models and real world situations. In effect, such models act as social laboratories incorporating human agency and feedback often difficult to quantify. The policymaker then benefits from the probabilistic spectrum of potential results derived from model outputs of different policy actions.

The negotiators realized that US positions on arms reductions reveal significant information on US arms and prospective technology advances. Also, unfortunately, the use of US intelligence in negotiations reveals the extent of this intelligence. The game theorists addressed the value and use of intelligence, behavior under repeated engagements, uncertainties about adversary's motives, technology innovation, and signaling intentions.

Today, Game Theory is the analytical engine for a wide range of National Security applications: securing airports (Assistance for Randomized Monitoring Over Routes; ARMOR), securing ports (Port Resilience Operational/Tactical Enforcement to Combat Terrorism; PROTECT), and assigning federal marshals to flights (Intelligent Randomization in Scheduling; IRIS).[22] These models effectively align limited security forces to threats prioritized by intelligence. The models analytic engine employs Bayesian Stackelberg Games which realistically simulate attacker-defender scenarios. In a Stackelberg Game the attacker surveys the target before mounting an attack on a hopefully inadequately defended target. The defender, aware of the attackers' surveillance, randomizes the deployment of defenders. The uncertainty of the attackers' approach and motivation is captured through a Bayesian approach of drawing the attacker from a random collection of adversaries. Intelligence on the attacker's objectives and operational approach is critical to model success.

Applying Risk Management Principles to Intelligence

There is a vigorous open debate on intelligence failures spanning what Thomas Fingar, the first Deputy Director of National Intelligence for Analysis

[20]John C. Harsanyi, 'Games with Incomplete Information', Nobel Lecture, 9 December 1994. < http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.136.9804&rep = rep1&type = pdf > (accessed 20 September 2013).

[21]Robert Aumann and Michael Maschler, *Repeated Games with Incomplete Information* (Cambridge: The MIT Press 1995).

[22]Tambe, *Security and Game Theory Algorithms*.

and former Chairman of the National Intelligence Council, expressed as: the fatal flaws of the 'error-plagued 2002 National Intelligence Estimate (NIE) on Iraq's weapons of mass destruction programs' to a 'no fault' view of intelligence where the policy community always escapes accountability through attributing their failures to intelligence failures.[23] His process-focused analysis, and the analytics and risk management process we propose, offer a more nuanced and constructive account guiding the application of change.

Fingar's observation is that intelligence analysis is estimative, all too often assessing future 'worst states' of events. Far too little analysis is devoted to opportunities of 'bending' the trajectory of events is valid if taken in the absence of a probabilistic framework. He offers examples on North Korean nuclear development. The efficacy of sanctions and rewards associated with diplomatic approaches are often marginalized by focusing on worst case scenarios and relegating alternate scenarios to the footnotes of an estimate. Our approach, encompassing complexity, human agency, and uncertainty, solves three additional problems.

First (consequences): The success of the models and forecasts previously discussed was enabled by rich historical data sets. This data quantified both the probability of events and their significant consequences. Unfortunately intelligence analysis often conflates uncertainty of the event with confidence in the estimate, tends to collapse analysis onto one future state, and does little to quantify consequences.

Second (human agency): Given an intelligence forecast, human agency, unlike the physical analogues discussed, can alter the path. Both US actions and the actions of our adversaries can significantly alter the trajectory of future events invalidating an intelligence assessment focused on one future state.

Third (contingency): We simply do not acknowledge that the consequences of our actions are not deterministic, and often contain significantly undesirable and unanticipated effects.

The IC has made progress on uncertainty through Intelligence Community Directive (ICD) 203: Analytic Standards.[24] Each of the Agencies has established training and review boards to enforce tradecraft. Tradecraft is focused on establishing the reliability of sources, expressing uncertainty or confidence in analytical judgments, distinguishing underlying intelligence from analyst's assumptions and judgments, and incorporating alternate analysis.

However, the realities of the intelligence process preclude the specification of multiple future states with attendant probabilities, and concerns over politizing intelligence tend to reserve the framing of consequences to policymakers. Conscientious analysts who frame alternative states are often faulted for 'your analysis is all over the map' or 'be decisive and make a choice'.

[23]Fingar, *Reducing Uncertainty* (Stanford: Stanford University Press 2011).

[24]Intelligence Community Directive Number 203: Analytic Standards, June 2007, <http://www.fas.org/irp/dni/icd/icd-203.pdf> (accessed 20 September 2013).

Daron Acemoglu and James Robinson provide insights on the problems of contingency and human agency raised above. In *Why Nations Fail*[25] they develop the political, economic, and historical factors that shape the rise and fall of nations.

The authors demonstrate the structure of their argument when discussing the timing of events. They attribute the divergent paths of history to small institutional differences influencing actions at critical junctures. Neither the actions nor their efficacy are predictable. Moreover, the critical junctions are ephemeral, meaning action delayed is opportunity lost. The authors' memorable term for this evolution is 'the contingent path of history'. They caution against reading history backwards to uncover an inevitable path forward.

It is unrealistic, and perhaps undesirable, to alter the process generating current intelligence to require alternate future states, their respective probabilities, and a measure of their consequence. The solution we propose is risk management coupled with agent-based modeling. This would prove effective at analyzing existing intelligence products to: (1) Refine probabilities and assign consequences to existing intelligence products, (2) Develop and evaluate an agent-based model across a broad community, (3) Continuously evaluate and adjust event probabilities and consequence measures, (4) Search for causal factors, and (5) Test the system through Stress Scenarios. This process would be a more formal approach to the Director's mandated Annual Risk Assessment with the added advantage of a vetted model to assist the process of adjusting IC objectives and resources to evolving threats.

The Challenge of Complexity

With the IRTPA reforms and subsequent Office of the Director of National Intelligence (ODNI) mandate for a more scientific approach to intelligence analysis we have witnessed a surge in techniques emphasizing the scientific method, many of which are fundamentally built on the idea that systems are complicated but not complex.[26] This introduces an important distinction when discussing the interconnected and interacting systems of human agency mentioned above. In a complicated system, one is able to predict and characterize the system as a whole by perfectly understanding the governing behavior of each component part (no matter how small). This assumed property of natural systems dominated nineteenth-century scientific thought. Although this scientific worldview changed at the turn of the twentieth century, the esoteric mathematics and the counterintuitive probabilistic nature of developing theories did not filter to the public or the Intelligence Community. As a result, the belief remains in both the public and the IC that although our universe is complicated it remains deterministic and subject to control.

[25]Daron Acemoglu and James A. Robinson, *Why Nations Fail: The Origins of Power, Prosperity, and Poverty* (NY: Crown Business 2012).

[26]Office of the Deputy Director of National Intelligence: Analytic Integrity and Standards, *Analytic Transformation – Unleashing the Potential of a Community of Analysts* (Washington, DC: Government Printing Office 2008).

Complexity theory formally challenges this belief. In complexity, the interdependent behavior of connected, heterogeneous, and adaptive elements frequently results in emergent macroscopic features not predictable from fundamental laws. Although the concepts underlying complexity are not new (such as the frequently cited 'invisible hand' introduced in the *Wealth of Nations* by Adam Smith who described how well-defined order emerged from the social behavior of butchers, brewers, and bakers[27]) more formalized development had to await the theoretical constructs and advanced computing capabilities of the last decade.[28]

Understanding Complex Networks through Agent-Base Modeling

After the dissolution of the Soviet Union and the 9/11 attacks, the model for US intelligence veered from a two-agent model (Figure 5, left) to a network model encompassing a greater number of adversaries (Figure 5, right). In Figure 5 the USA (large circle) and the Soviet Union are represented by the black circles with the cold war bi-polar world bounding the number of actors. With the disintegration of the Soviet Union, the IC became increasingly concerned with a growing number of adversaries that included growing countries with nuclear weapons (successors to the Soviet Union), rogue nations such as North Korea, dysfunctional countries such as Afghanistan, and sprawling terrorist networks. Figure 5 (right) reinforces the point that network complexity increases with both the number of agents and the connectivity between agents.

Complexity problems require the talents of a diverse group of professionals and are addressed at multi-disciplinary centers such as the Santa Fe Institute and the University of Michigan. The IC can benefit from this approach through adopting the analytics and drawing on outside resources to model a diverse set of problems.

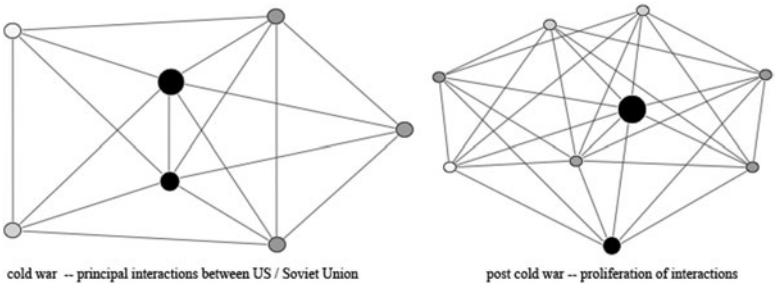

Figure 5. Network Complexity from Increased Agents and Linkages.

[27]Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations* (London: W. Strahan and T. Cadell, 1776) <http://www2.hn.psu.edu/faculty/jmanis/adam-smith/wealth-nations.pdf> (accessed 20 September 2013) p.364.
[28]John H. Miller and Scott E. Page, *Complex Adaptive Systems* (Princeton: Princeton University Press 2007) p.26.

Figure 6. The Hive from the Long Baseline Neutrino Experiment which shows the conceptual construct for a collaboration from 58 different institutions.[29]

Unmet expectations from the 9/11 and WMD Commissions are unity of effort stretching beyond the Intelligence Community, and quick, imaginative, and agile response to threats. Corporations have always exploited innovations, processes, and technologies from the outside, through joint ventures and patents and processes from academia. The IC should move towards a distributed resource model and away from resources concentrated in Agency fortresses. This will accelerate the progress made on internal collaboration while enabling broader outside collaboration.

Over the last 30 years corporations have steadily moved resources from headquarters to the field. The IC has validated that model through the success of deploying Intelligence resources with the warfighter. A goal to emulate is the 300-plus collaborators from 58 institutions across the US, India, Italy, Japan, and the UK planning and designing the US$900 million Long Baseline Neutrino Experiment.[30] This project team uses the analogy of a bee colony to model coordination and interactions. A bee colony is so highly integrated and flawlessly choreographed that it operates as a single organism.

Thomas Fingar dedicated a chapter of his recent book to the neglected role of intelligence to anticipate opportunities and shape the future.[31] An Intelligence Community better able to estimate the potential influence of both policymaker and adversary decisions will be better poised to prevent black swan events and reduce the chances of future intelligence failures.

[29]Amelia Smith, 'LBNE: The Inside Buzz on a Science Project', *Symmetry: Dimensions of Particle Physics* 8/2 (2011), < http://www.symmetrymagazine.org/sites/default/files/legacy/pdfs/201105/lbne_the_inside_buzz.pdf> (accessed 20 September 2013) pp.18–23.
[30]Ibid.
[31]Thomas Fingar, *Reducing Uncertainty* (Stanford: Stanford University Press 2011).

By enlarging the set of questions and hypothetical situations that may be posed, agent-based modeling permits us to productively explore and investigate the potential influences of path-dependent decisions by key agents. Such models would help to focus funding and efforts where the largest intelligence benefits might be realized by identifying regions where the policy maker may anticipate opportunities and shape the future. These models might be used to help explore a system's robustness to both random and strategic attack.[32]

Fortunately, the IC will not be undertaking this effort from scratch. Several related fields (such as economics[33] and sociology[34]) have forged the path when it comes to agent-based modeling.[35] The fundamental principles underlying computer science, economics, and other social science models will provide a starting point for Intelligence Community agent-based models.[36]

Finally, there is a need to test scenarios in a simulated environment to identify the potential influences of different human agency actions. In effect, the Intelligence Community needs a virtual laboratory to play out path-dependent decisions and interactions with a focus on obtaining a better understanding of the influences agents have within a given system instead of trying to control it.[37] Unfortunately, in spite of the successes enumerated above and a body of academic social science work on terrorist networks,[38] complexity theory has not been embraced by the Intelligence Community. The authors' next paper will develop an agent-based model for intelligence warning by forecasting alternate futures of fragile states. Fragile states lack the capacity to provide basic social services and security to their citizens. These deficiencies spawn conflict, trafficking, organized crime, and terrorism to bordering states and the world proliferating possible intelligence outcomes.

Conclusions

After highlighting the role of uncertainty and expanding on the notion that events in the real world are path-dependent and contingent on deterministic and random elements, we have shown how human agency in an interconnected and

[32]Sergey V. Buldyrev, Roni Parshani, Gerald Paul, H. Eugene Stanley, and Shlomo Havlin, 'Catastrophic Cascade of Failures in Interdependent Networks', *Nature* 464 (2010) pp.1025–8.
[33]Ken Kollman, John H. Miller, and Scott E. Page, 'Political Institutions and Sorting in the Tiebout Model', *American Economic Review* 87 (1997) pp.977–92.
[34]Mark Grannoveter, 'Threshold Models of Collective Behavior', *American Journal of Sociology* 83 (1978) pp.1420–3; see also Susanne Lohmann, 'A Signaling Model of Information and Manipulative Political Action', *American Political Science Review* 88 (1993) pp.319–33.
[35]Scott E. Page, 'On Incentives and Updating in Agent-Based Models', *Computational Economics* 10 (1997) pp.67–87.
[36]Sanjeev Arora and Boaz Barak, *Computational Complexity* (NY: Cambridge University Press 2009).
[37]Yang-Yu Liu, Jean-Jacques Slotine, and Albert-Laszlo Barabasi, 'Controllability of Complex Networks', *Nature* 473 (2011) pp.167–73.
[38]Nancy K. Hayden, 'The Complexity of Terrorism: Social and Behavioral Understanding', in Magnus Ranstorp (ed.) *Mapping Terrorism Research* (London: Routledge 2007) p.292.

interdependent system can lead to a landscape of dancing strategies as agents dynamically modify their responses to different events. We emphasize how the current overly deterministic approach of the IC introduces a significant adjustment lag (or time delay) on the order of 10 years.

The dissolution of the Soviet Union challenged the traditional two-agent threat model of the cold war as threats emanating from multiple directions began to emerge. Although the risk of intelligence failures will always be present, in the years following large geopolitical shifts vulnerability to them increases. In an analyst-centric system this inherent adjustment time compounded by complex behavior, bolsters the potential for catastrophic emergent threats, and significantly elevates the probability of future intelligence failures.

An era complicated by nuclear proliferation, the Arab Spring, the rapid rise of Chinese power, an oil-fueled Russian resurgence, and post-Afghan and Iraq will demand significant changes in intelligence focus, processes, and resources. Meeting this challenge requires a *community intelligence process* drawing on theory, models, and resources outside the community. Adopting this community intelligence process requires a paradigm shift in the distribution of responsibilities, work, and analytic tools of the Intelligence Community. The model for this transformation is available from fields as diverse as biology, economics, sociology, and physics. By adopting a process-oriented approach to analysis with a foundation in uncertainty, game theory, and complexity we can radically reduce the adjustment lag to emerging threats while reducing our vulnerability to black swan events.

Disclaimer

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the Department of Defense, the Defense Intelligence Agency, the National Intelligence University, the US Air Force, or the US Government.

Notes on Contributors

Dr Daniel Javorsek II is a Major in the US Air Force and a graduate student at the National Intelligence University (NIU). Since receiving his PhD in Physics from Purdue University in 2001 he has been a regular consumer of intelligence, initially as an operational F-16 pilot and more recently as an F-22 experimental test pilot.

Mr John G. Schwitz is an executive with a successful track record of restructuring organizations to high-performance at radically reduced costs. He is currently the Program Manager for the implementation of a suite of cybersecurity products across the Intelligence Community. His paper 'Risk Based Cybersecurity Policy' was published in June 2011, and 'Assuring The Intelligence Base Through Governance, Benchmarking, and Common Services' will be published in 2013, both in *American Intelligence Journal*.